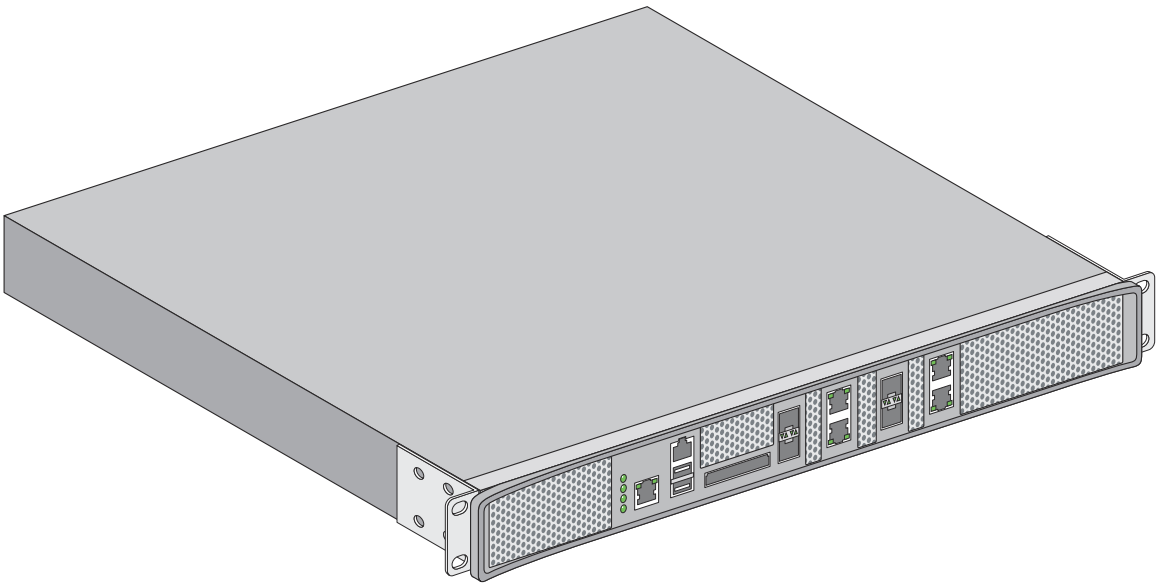
Motorola Solutions RFS7000GR Series RF Switch

CLI Reference Guide



MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2014 Motorola Solutions, Inc. All rights reserved.

Table of Contents

About This Guide

Who Should Use this Guide **1-13**
How to Use this Guide **1-13**
Conventions Used in this Guide **1-15**
Annotated Symbols 1-15
Notational Conventions 1-15
Motorola Solutions Service Information **1-17**
Product Sales and Product Information 1-17
General Information 1-17
Motorola Solutions, Inc.
End-User License Agreement1-18

Chapter 1. Introduction

1.1 Common Criteria Operational Requirements **1-1**
1.1.1 Configuration of MAC ACL For Common Criteria Operation 1-2
1.1.2 Configuration of IP ACL For Common Criteria Operation 1-5
1.2 CLI Overview **1-7**
1.3 Getting Context Sensitive Help **1-9**
1.4 Using the no and default forms of Commands **1-11**
1.5 Setting the Administrator Inactivity Timeout **1-11**
1.6 Basic Conventions **1-11**
1.7 Using CLI Editing Features and Shortcuts **1-11**
1.7.1 Moving the Cursor on the Command Line 1-11
1.7.2 Completing a Partial Command Name 1-12
1.7.3 Deleting Entries 1-13
1.7.4 Re-displaying the Current Command Line 1-13
1.7.5 Command Output pagination 1-13
1.7.6 Transposing Mistyped Characters 1-14
1.7.7 Controlling Capitalization 1-14

Chapter 2. Common Commands

2.1 Common Commands **2-1**
2.1.1 clrscr 2-2
2.1.2 exit 2-3
2.1.3 help 2-4
2.1.4 no 2-6
2.1.5 service 2-8
2.1.6 show 2-25

2.1.7 aap-wlan-acl 2-28
2.1.8 aap-wlan-acl-stats 2-29
2.1.9 access-banner 2-30
2.1.10 audit-log-filters 2-31
2.1.11 autoinstall 2-32
2.1.12 commands 2-33
2.1.13 crypto 2-34
2.1.14 crypto-error-log 2-36
2.1.15 crypto-log 2-37
2.1.16 environment 2-38
2.1.17 firewall 2-39
2.1.18 history 2-40
2.1.19 interfaces 2-41
2.1.20 ip 2-43
2.1.21 ldap 2-48
2.1.22 licenses 2-49
2.1.23 logging 2-50
2.1.24 mac 2-51
2.1.25 mac-address-table 2-52
2.1.26 mac-name 2-53
2.1.27 management 2-54
2.1.28 mobility 2-55
2.1.29 ntp 2-57
2.1.30 port 2-58
2.1.31 port-channel 2-59
2.1.32 privilege 2-60
2.1.33 protocol-list 2-61
2.1.34 radius 2-62
2.1.35 redundancy 2-63
2.1.36 role 2-64
2.1.37 rtls 2-65
2.1.38 service-list 2-67
2.1.39 smtp-notification 2-68
2.1.40 snmp 2-69
2.1.41 snmp-server 2-70
2.1.42 spanning-tree 2-71
2.1.43 static-channel-group 2-73
2.1.44 terminal 2-74
2.1.45 timezone 2-75
2.1.46 traffic shape 2-76
2.1.47 users 2-77
2.1.48 version 2-78
2.1.49 virtual ip 2-79
2.1.50 wireless 2-80
2.1.51 wlan-acl 2-90
2.1.52 access-list 2-91
2.1.53 aclstats 2-92
2.1.54 boot 2-93
2.1.55 clock 2-94
2.1.56 debugging 2-95

2.1.57 dhcp 2-96
2.1.58 file 2-97
2.1.59 password-encryption 2-98
2.1.60 running-config 2-99
2.1.61 securitymgr 2-100
2.1.62 sessions 2-101
2.1.63 startup-config 2-102
2.1.64 upgrade-status 2-103
2.1.65 wlan-acl 2-104

Chapter 3. User Exec Commands

3.1 User Exec Commands 3-1
3.1.1 clear 3-3
3.1.2 cluster-cli 3-4
3.1.3 disable 3-5
3.1.4 enable 3-6
3.1.5 logout 3-7
3.1.6 page 3-8
3.1.7 ping 3-9
3.1.8 quit 3-10
3.1.9 show 3-11
3.1.10 terminal 3-14
3.1.11 traceroute 3-15

Chapter 4. Privileged Exec Commands

4.1 Priv Exec Commands 4-1
4.1.1 acknowledge 4-3
4.1.2 archive 4-4
4.1.3 change-passwd 4-6
4.1.4 clear 4-7
4.1.5 clock 4-11
4.1.6 cluster-cli 4-12
4.1.7 configure 4-13
4.1.8 copy 4-14
4.1.9 disable 4-15
4.1.10 enable 4-16
4.1.11 erase 4-17
4.1.12 halt 4-18
4.1.13 keytransfer 4-19
4.1.14 logout 4-20
4.1.15 page 4-21
4.1.16 ping 4-22
4.1.17 pwd 4-23
4.1.18 quit 4-24
4.1.19 reload 4-25
4.1.20 run 4-26
4.1.21 show 4-27
4.1.22 terminal 4-45

4.1.23 traceroute 4-46
4.1.24 upgrade 4-47
4.1.25 upgrade-abort 4-48
4.1.26 write 4-49

Chapter 5. Global Configuration Commands

5.1 Global Configuration Commands 5-1
5.1.1 aaa 5-4
5.1.2 aap-wlan-acl 5-5
5.1.3 access-banner 5-6
5.1.4 access-list 5-7
5.1.5 arp 5-14
5.1.6 audit-log-filter 5-15
5.1.7 auth-timeout 5-17
5.1.8 autoinstall 5-18
5.1.9 boot 5-19
5.1.10 bridge 5-20
5.1.11 country-code 5-22
5.1.12 crypto 5-23
5.1.13 do 5-28
5.1.14 end 5-29
5.1.15 errdisable 5-30
5.1.16 firewall 5-31
5.1.17 hostname 5-33
5.1.18 interface 5-34
5.1.19 ip 5-35
5.1.20 license 5-44
5.1.21 line 5-45
5.1.22 local 5-46
5.1.23 logging 5-47
5.1.24 mac 5-49
5.1.25 mac-address-table 5-50
5.1.26 mac-name 5-51
5.1.27 management 5-52
5.1.28 network-element-id 5-53
5.1.29 ntp 5-54
5.1.30 prompt 5-58
5.1.31 radius-server 5-59
5.1.32 ratelimit 5-60
5.1.33 redundancy 5-61
5.1.34 remote-login 5-64
5.1.35 role 5-65
5.1.36 rtls 5-66
5.1.37 service 5-67
5.1.38 show 5-70
5.1.39 smtp-notification 5-83
5.1.40 snmp-server 5-85
5.1.41 spanning-tree 5-87
5.1.42 timezone 5-89

5.1.43 traffic-shape 5-90
5.1.44 username 5-91
5.1.45 virtual-ip 5-92
5.1.46 vpn 5-94
5.1.47 wireless 5-95
5.1.48 wlan-acl 5-96
5.1.49 zeroize 5-98

Chapter 6. Crypto - isakmp Instance

6.1 Crypto ISAKMP Config Commands 6-1
6.1.1 authentication 6-2
6.1.2 clrscr 6-3
6.1.3 encryption 6-4
6.1.4 end 6-5
6.1.5 exit 6-6
6.1.6 hash 6-7
6.1.7 help 6-8
6.1.8 lifetime 6-9
6.1.9 no 6-10
6.1.10 service 6-11
6.1.11 show 6-12

Chapter 7. Crypto - group Instance

7.1 Crypto Group Config Commands 7-1
7.1.1 clrscr 7-2
7.1.2 dns 7-3
7.1.3 end 7-4
7.1.4 exit 7-5
7.1.5 help 7-6
7.1.6 service 7-7
7.1.7 show 7-8
7.1.8 wins 7-10

Chapter 8. Crypto - peer Instance

8.1 Crypto Peer Config Commands 8-1
8.1.1 clrscr 8-2
8.1.2 end 8-3
8.1.3 exit 8-4
8.1.4 help 8-5
8.1.5 no 8-6
8.1.6 service 8-7
8.1.7 set 8-8
8.1.8 show 8-9

Chapter 9. Crypto - ipsec Instance

9.1 Crypto IPSec Config Commands 9-1

9.1.1 clrscr 9-2
9.1.2 end 9-3
9.1.3 exit 9-4
9.1.4 help 9-5
9.1.5 mode 9-6
9.1.6 no 9-7
9.1.7 service 9-8
9.1.8 show 9-9

Chapter 10. Crypto - map Instance

10.1 Crypto Map Config Commands 10-1
10.1.1 clrscr 10-2
10.1.2 end 10-3
10.1.3 exit 10-4
10.1.4 help 10-5
10.1.5 match 10-6
10.1.6 no 10-7
10.1.7 service 10-8
10.1.8 set 10-9
10.1.9 show 10-12

Chapter 11. Crypto - trustpoint Instance

11.1 Trustpoint Config commands 11-1
11.1.1 clrscr 11-2
11.1.2 company-name 11-3
11.1.3 email 11-4
11.1.4 end 11-5
11.1.5 exit 11-6
11.1.6 fqdn 11-7
11.1.7 help 11-8
11.1.8 ip-address 11-9
11.1.9 no 11-10
11.1.10 password 11-11
11.1.11 rsakeypair 11-12
11.1.12 service 11-13
11.1.13 show 11-14
11.1.14 subject-name 11-16

Chapter 12. Interface Instance

12.1 Interface Config commands 12-1
12.1.1 clrsc r12-3
12.1.2 crypto 12-4
12.1.3 description 12-5
12.1.4 duplex 12-6
12.1.5 end 12-7
12.1.6 exit 12-8
12.1.7 help 12-9

12.1.8 ip 12-10
12.1.9 mac 12-12
12.1.10 management 12-13
12.1.11 no 12-14
12.1.12 port-channel 12-15
12.1.13 service 12-16
12.1.14 show 12-17
12.1.15 shutdown 12-19
12.1.16 spanning-tree 12-20
12.1.17 speed 12-22
12.1.18 static-channel-group 12-23
12.1.19 switchport 12-24
12.1.20 storm-control 12-26

Chapter 13. Spanning Tree-MST Instance

13.1 MST Config commands 13-1
13.1.1 clrscr 13-2
13.1.2 end 13-3
13.1.3 exit 13-4
13.1.4 help 13-5
13.1.5 instance 13-6
13.1.6 name 13-7
13.1.7 no 13-8
13.1.8 revision 13-9
13.1.9 service 13-10
13.1.10 show 13-11
13.2 Configuring Interface using MSTP 13-12

Chapter 14. Extended ACL Instance

14.1 Extended ACL Config Commands 14-1
14.1.1 clrscr 14-2
14.1.2 deny 14-3
14.1.3 end 14-8
14.1.4 exit 14-9
14.1.5 help 14-10
14.1.6 mark 14-11
14.1.7 no 14-17
14.1.8 permit 14-18
14.1.9 service 14-24
14.1.10 show 14-25

Chapter 15. Standard ACL Instance

15.1 Standard ACL Config Commands 15-1
15.1.1 clrscr 15-2
15.1.2 deny 15-3
15.1.3 end 15-4
15.1.4 exit 15-5

15.1.5 help 15-6
15.1.6 mark 15-7
15.1.7 no 15-8
15.1.8 permit 15-9
15.1.9 service 15-10
15.1.10 show 15-11

Chapter 16. Extended MAC ACL Instance

16.1 MAC Extended ACL Config Commands 16-1
16.1.1 clrscr 16-2
16.1.2 deny 16-3
16.1.3 end 16-6
16.1.4 exit 16-7
16.1.5 help 16-8
16.1.6 mark 16-9
16.1.7 no 16-11
16.1.8 permit 16-12
16.1.9 service 16-15
16.1.10 show 16-16

Chapter 17. DHCP Instance

17.1 DHCP Config Commands 17-1
17.1.1 address 17-3
17.1.2 bootfile 17-4
17.1.3 class 17-5
17.1.4 client-identifier 17-10
17.1.5 client-name 17-11
17.1.6 clrscr 17-12
17.1.7 ddns 17-13
17.1.8 default-router 17-14
17.1.9 dns-server 17-15
17.1.10 domain-name 17-16
17.1.11 end 17-17
17.1.12 exit 17-18
17.1.13 hardware-address 17-19
17.1.14 help 17-20
17.1.15 host 17-21
17.1.16 lease 17-22
17.1.17 netbios-name-server 17-23
17.1.18 netbios-node-type 17-24
17.1.19 network 17-25
17.1.20 next-server 17-26
17.1.21 no 17-27
17.1.22 option 17-28
17.1.23 service 17-29
17.1.24 show 17-30
17.1.25 unicast-enable 17-32
17.1.26 update 17-33

17.2 Configuring DHCP Server using CLI 17-34
17.2.1 Creating network pool 17-35
17.2.2 Creating host pool 17-36
17.2.3 Troubleshooting DHCP configuration 17-37

Chapter 18. DHCP Class Instance

18.1 DHCP Server Class Config Commands 18-1
18.1.1 clrscr 18-2
18.1.2 end 18-3
18.1.3 exit 18-4
18.1.4 help 18-5
18.1.5 multiple-user-class 18-6
18.1.6 no 18-7
18.1.7 option 18-8
18.1.8 service 18-9
18.1.9 show 18-10

Chapter 19. RADIUS Server Instance

19.1 RADIUS Configuration Commands 19-1
19.1.1 authentication 19-3
19.1.2 ca 19-4
19.1.3 clrscr 19-5
19.1.4 crl-check 19-6
19.1.5 end 19-7
19.1.6 exit 19-8
19.1.7 group 19-9
19.1.8 help 19-27
19.1.9 ldap-group-verification 19-28
19.1.10 ldap-server 19-29
19.1.11 nas 19-31
19.1.12 no 19-32
19.1.13 proxy 19-33
19.1.14 rad-user 19-34
19.1.15 server 19-36
19.1.16 service 19-37
19.1.17 show 19-38

Chapter 20. Wireless Instance

20.1 Wireless Configuration Commands 20-1
20.1.1 aap 20-4
20.1.2 admission-control 20-6
20.1.3 adopt-unconf-radio 20-7
20.1.4 adoption-pref-id 20-8
20.1.5 ap 20-9
20.1.6 ap-containment 20-11
20.1.7 ap-detection 20-12
20.1.8 ap-image 20-14

20.1.9 ap-ip 20-15
20.1.10 ap-standby-attempts-threshold 20-16
20.1.11 ap-timeout 20-17
20.1.12 auto-select-channels 20-18
20.1.13 broadcast-tx-speed 20-19
20.1.14 client 20-20
20.1.15 clrscr 20-31
20.1.16 cluster-master-support 20-32
20.1.17 country-code 20-33
20.1.18 debug 20-34
20.1.19 dhcp-one-portal-forward 20-36
20.1.20 dhcp-sniff-state 20-37
20.1.21 dot11k 20-38
20.1.22 end 20-39
20.1.23 exit 20-40
20.1.24 fix-broadcast-dhcp-rsp 20-41
20.1.25 hotspot 20-42
20.1.26 help 20-43
20.1.27 load-balance 20-44
20.1.28 mac-auth-local 20-45
20.1.29 manual-wlan-mapping 20-47
20.1.30 mobile-unit 20-48
20.1.31 mobility 20-49
20.1.32 multicast-packet-limit 20-50
20.1.33 multicast-throttle-watermarks 20-51
20.1.34 nas-id 20-52
20.1.35 nas-port-id 20-53
20.1.36 non-preferred-ap-attempts-threshold 20-54
20.1.37 no 20-55
20.1.38 proxy-arp 20-56
20.1.39 qos-mapping 20-57
20.1.40 radio 20-58
20.1.41 rate-limit 20-68
20.1.42 self-heal 20-69
20.1.43 sensor 20-70
20.1.44 service 20-71
20.1.45 smart-rf 20-78
20.1.46 show 20-79
20.1.47 smart-scan-channels 20-81
20.1.48 test 20-82
20.1.49 wips 20-83
20.1.50 wlan 20-87
20.1.51 wlan-bw-allocation 20-99

Chapter 21. RTLS Instance

21.1 RTLS Config Commands 21-1
21.1.1 aeroscout 21-2
21.1.2 ap 21-3
21.1.3 clrscr 21-4

21.1.4 end 21-5
21.1.5 exit 21-6
21.1.6 help 21-7
21.1.7 ekahau 21-8
21.1.8 no 21-9
21.1.9 service 21-11
21.1.10 show 21-13
21.1.11 site 21-15
21.1.12 sole 21-17
21.1.13 switch 21-18

Chapter 22. Role Instance

22.1 Role Config Commands 22-1
22.1.1 ap-location 22-3
22.1.2 authentication-type 22-4
22.1.3 encryption-type 22-5
22.1.4 essid 22-6
22.1.5 group 22-7
22.1.6 ip 22-8
22.1.7 mac 22-9
22.1.8 mu-mac 22-10
22.1.9 clrscr 22-11
22.1.10 no 22-12
22.1.11 end 22-13
22.1.12 exit 22-14
22.1.13 help 22-15
22.1.14 service 22-16
22.1.15 show 22-17

Chapter 23. Sole Instance

23.1 Sole Config Commands 23-1
23.1.1 aap-rssi-update-interval 23-2
23.1.2 clrscr 23-3
23.1.3 end 23-4
23.1.4 exit 23-5
23.1.5 help 23-6
23.1.6 locate 23-7
23.1.7 mobile-unit 23-8
23.1.8 no 23-9
23.1.9 redundancy 23-10
23.1.10 rssi-filter 23-11
23.1.11 service 23-12
23.1.12 show 23-13

Appendix A. Customer Support

About This Guide

This preface introduces the *Motorola Solutions RFS7000GR Series RF Switch CLI Reference Guide* and contains the following sections:

- *Who Should Use this Guide*
- *How to Use this Guide*
- *Conventions Used in this Guide*
- *Motorola Solutions Service Information*

Who Should Use this Guide

The *Motorola Solutions RFS7000GR Series RF Switch CLI Reference Guide* is intended for system administrators responsible for the implementing, configuring, and maintaining the RFS7000 using the switch *command line interface* (CLI). It also serves as a reference for configuring and modifying most common system settings. The administrator must be familiar with wireless technologies, network concepts, ethernet concepts, as well as IP addressing and SNMP concepts.

How to Use this Guide

This guide helps you implement, configure, and administer the RFS7000 Switch and associated network elements. This guide is organized into the following sections:

Table 1 Quick Reference on How This Guide Is Organized

Chapter	Jump to this section if you want to...
Chapter 1, Introduction	Review the overall feature-set of the RFS7000 Switch, as well as the many configuration options available.
Chapter 2, Common Commands	Summarize the commands common amongst many contexts and instance contexts within the RFS7000 Switch CLI.
Chapter 3, User Exec Commands	Summarize the User Exec commands within the RFS7000 Switch CLI.
Chapter 4, Privileged Exec Commands	Summarize the Priv Exec commands within the RFS7000 Switch CLI.
Chapter 5, Global Configuration Commands	Summarize the Global Config commands within the RFS7000 Switch CLI.

Table 1 Quick Reference on How This Guide Is Organized (Continued)

Chapter	Jump to this section if you want to...
Chapter 5, Global Configuration Commands	Summarize the crypto-isakmp commands within the RFS7000 Switch CLI.
Chapter 7, Crypto - group Instance	Summarize the crypto-group commands within the RFS7000 Switch CLI.
Chapter 8, Crypto - peer Instance	Summarize the crypto-peer commands within the RFS7000 Switch CLI.
Chapter 9, Crypto - ipsec Instance	Summarize the crypto-ipsec commands within the RFS7000 Switch CLI.
Chapter 10, Crypto - map Instance	Summarizes the crypto-map commands within the RFS7000 Switch CLI.
Chapter 11, Crypto - trustpoint Instance	Summarize the **(crypto-trustpoint)** commands within the RFS7000 Switch CLI.
Chapter 12, Interface Instance	Summarize the **(config-if)** commands within the RFS7000 Switch CLI.
Chapter 13, Spanning Tree-MST Instance	Summarize the **(config-mst)** commands within the RFS7000 Switch CLI.
Chapter 14, Extended ACL Instance	Summarize the **(config-ext-nacl)** commands within the RFS7000 Switch CLI.
Chapter 15, Standard ACL Instance	Summarize the **(config-std-nacl)** commands within the RFS7000 Switch CLI.
Chapter 16, Extended MAC ACL Instance	Summarize the **(config-ext-macl)** commands within the RFS7000 Switch CLI.
Chapter 17, DHCP Instance	Summarize the **(config-dhcp pool)** commands within the RFS7000 Switch CLI.
Chapter 18, DHCP Class Instance	Summarize the **(config-dhcp-class)** instance commands within the RFS7000 Switch CLI.
Chapter 19, RADIUS Server Instance	Summarize the **(config-radsrv)** instance commands within the RFS7000 Switch CLI.
Chapter 20, Wireless Instance	Summarize the **(config-wireless)** instance commands within the RFS7000 Switch CLI.
Chapter 21, RTLS Instance	Summarize the **(config-rtls)** instance commands within the RFS7000 Switch CLI.
Chapter 22, Role Instance	Summarize the **(config-role)** instance commands within the RFS7000 Switch CLI.
Chapter 23, Sole Instance	Summarize the **(config-sole)** instance commands within the RFS7000 Switch CL

Conventions Used in this Guide

This section describes the following topics:

- *Annotated Symbols*
- *Notational Conventions*

Annotated Symbols

The following document conventions are used in this document:

NOTE Indicates tips or special requirements.

CAUTION Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Table 2 Notational Convention used in the document

Convention	Example Token	Description	Valid Inputs
bold		Bold text indicates commands and keywords that you enter literally	
italics		Italic text indicates arguments for which you supply values.	
()	(on|off)	Grouping (exactly one of a list of tokens)	on
{}	{key1|key2|key3}	Selective recursive (multiple tokens allowed, but each can only be used once)	key1 key3

Table 2 Notational Convention used in the document

Convention	Example Token	Description	Valid Inputs
[ ]	[key1|key2|key3]	Infinite recursive (multiple tokens allowed, each can be used multiple times)	key1 key1 key2 key3 key2 key3
.	.<1-10>	Simple infinite recursive	1 2 6
?	[key1|?key2]	Selective keyword in infinite recursive.	key1 key1 key2

Motorola Solutions Service Information

Use the Motorola Solutions Support Center as the primary contact for any technical problem, question, or support issue involving Motorola Solutions products. Motorola Solutions Support Center responds to calls by e-mail, telephone or fax within the time limits set forth in individual contractual agreements:

Telephone (North America): 1-800-653-5350

Telephone (International): +1-631-738-6213

Fax: (631) 738-5410

E-mail: *https://portal.motorolasolutions.com/Support/US-EN*

When contacting Motorola Solutions Support Center, please provide the following information:

- Serial number of the unit.
- Model number or product name.
- Software type and version number.

Product Sales and Product Information

North America	International
Motorola Solutions, Inc. One Motorola Plaza Holtsville, New York 11742-1300 Tel: 1-631-738-2400 or 1-800-722-6234 Fax: 1-631-738-5990	Motorola Solutions, Inc. Symbol Place Winnersh Triangle, Berkshire, RG41 5TP United Kingdom Tel: 0800-328-2424 (Inside UK) +44 118 945 7529 (Outside UK)

General Information

For general information, contact Motorola Solutions at:

Telephone (North America): 1-800-722-6234

Telephone (International): +1-631-738-5200

Website: *http://www.motorolasolutions.com*

Motorola Solutions, Inc.
End-User License Agreement

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE DESCRIBED IN THIS DOCUMENT, YOU OR THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT"). LICENSEE'S USE OR CONTINUED USE OF THE DOWNLOADED OR INSTALLED MATERIALS SHALL ALSO CONSTITUTE ASSENT TO THE TERMS OF THIS AGREEMENT. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUTE THE INSTALLATION PROCESS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO AND EXPRESSLY CONTINGENT UPON THESE TERMS. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF A COMPANY, ANOTHER PERSON OR ANY OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THAT COMPANY, PERSON OR ENTITY.

1. LICENSE GRANT. Subject to the terms of this Agreement, Motorola Solutions, Inc. and/or its subsidiaries ("Licensor") hereby grants Licensee a limited, personal, non-sublicensable, non transferable, nonexclusive license to use the software that Licensee is about to download or install and the documentation that accompanies it (collectively, the "Software") for Licensee's personal use in connection with hardware produced by Licensor and only in accordance with the accompanying documentation. Licensee may download, install and use the Software only on a single computer. Licensee may make one copy of the Software (excluding any documentation) for backup purposes, provided that copyright and other restricted rights notices of Licensor and its suppliers are reproduced exactly.
2. LICENSE RESTRICTIONS. Except as expressly permitted by this Agreement, Licensee shall not, nor permit anyone else to, directly or indirectly: (i) copy (except for one backup copy), modify, distribute or create derivative works based upon the Software; (ii) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or structure, sequence and organization of the Software; or (iii) rent, lease, or use the Software for timesharing or service bureau purposes, or otherwise use the Software for any commercial purpose/on behalf of any third party. Licensee shall maintain and not remove or obscure any proprietary notices on the Software, and shall reproduce such notices exactly on all permitted copies of the Software. All title, ownership rights, and intellectual property rights in and to the Software, and any copies or portions thereof, shall remain in Licensor and its suppliers or licensors. Licensee understands that Licensor may modify or discontinue offering the Software at any time. The Software is protected by the copyright laws of the United States and international copyright treaties. The Software is licensed, not sold. This Agreement does not give Licensee any rights not expressly granted herein.
3. INTELLECTUAL PROPERTY; CONTENT. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Software), and any copies you are permitted to make herein are owned by Licensor or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. As a condition to Licensee's use of the Software, Licensee represents, warrants and covenants that Licensee will not use the Software: (i) to infringe the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party; (ii) to violate any applicable law, statute, ordinance or regulation; (iii) to disseminate information or materials in any form or format ("Content") that are harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or (iv) to disseminate any software viruses or any other computer code, files or programs that mayinterrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment. Licensee, not Licensor, remains solely responsible for all Content that Licensee uploads, posts, e-mails, transmits, or otherwise disseminates using, or in connection with, the Software.

4. FEES; SUPPORT AND UPGRADES. Licensor may, at Licensor's sole option, provide support services related to the Software ("Support Services"). Nothing in this Agreement grants Licensee any right to receive any Support Services. Use of any Support Services provided is governed by the Licensor policies and programs described in the user manual, in "online" documentation, and/or in other Licensor-provided materials or support agreements. Any supplemental software code provided to you as part of any Support Services shall be considered part of the Software and subject to the terms and conditions of this EULA. With respect to technical information you provide to Licensor as part of any Support Services, Licensor may use such information for its business purposes, including for product support and development. Licensor will not utilize such technical information in a form that personally identifies Licensee.
5. TERMINATION. Either party may terminate this Agreement at any time, with or without cause, upon written notice. Any termination of this Agreement shall also terminate the licenses granted hereunder. Upon termination of this Agreement for any reason, Licensee shall return all copies of the Software to Licensor, or destroy and remove from all computers, hard drives, networks, and other storage media all copies of the Software, and shall so certify to Licensor that such actions have occurred. Sections 2-13 shall survive termination of this Agreement.
6. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Licensor and its suppliers provide the Software and any (if any) Support Services AS IS AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability, of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of workmanlike effort, all with regard to the Software, and the provision of or failure to provide Support Services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NONINFRINGEMENT WITH REGARD TO THE SOFTWARE. THE ENTIRE RISK AS TO THE QUALITY OF OR ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE AND SUPPORT SERVICES, IF ANY, REMAINS WITH LICENSEE.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY GENERAL, SPECIAL, INCIDENTAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF LICENSOR OR ANY SUPPLIER, AND EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
8. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that Licensee might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Licensor and any of its suppliers under any provision of this Agreement and Licensee's exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by Licensee for the Software or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

9. INDEMNITY. Licensee agrees that Licensor shall have no liability whatsoever for any use Licensee makes of the Software. Licensee shall indemnify and hold harmless Licensor from any claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from Licensee's use of the Software as well as from Licensee's failure to comply with any term of this Agreement.
10. FAULT TOLERANCE. The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale in on-line control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to, the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, life support machines, or weapons systems, in which the failure of the Software could lead directly or indirectly to death, personal injury, or physical or environmental damage ("High Risk Activities"). Licensor and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.
11. U.S. GOVERNMENT LICENSE RIGHTS. Software provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. Software provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227- 7013 (OCT 1988), as applicable. The "Manufacturer" for purposes of these regulations is Motorola Solutions, Inc., One Symbol Plaza, Holtsville, NY 11742.
12. EXPORT RESTRICTIONS. Licensee shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and Licensee shall not export, or allow the export or re-export of the Software in violation of any such restrictions, laws or regulations. By downloading or using the Software, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any restricted country.
13. MISCELLANEOUS. Licensee may not sublicense, assign, or transfer this Agreement, or its rights or obligations hereunder, without the prior written consent of Licensor. Any attempt to otherwise sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is null and void. Licensor may assign this Agreement in its sole discretion. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. No waiver or modification of this Agreement will be binding upon a party unless made in writing and signed by a duly authorized representative of such party and no failure or delay in enforcing any right will be deemed a waiver. This Agreement shall be governed by the laws of the State of New York without regard to the conflicts of law provisions thereof. The application the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Unless waived by Licensor for a particular instance, any action or proceeding arising out of this Agreement must be brought exclusively in the state or federal courts of New York and Licensee hereby consents to the jurisdiction of such courts for any such action or proceeding. This Agreement supersedes all prior discussions and writings and constitutes the entire agreement between the parties with respect to the subject matter hereof. The prevailing party in any action arising out of this Agreement shall be entitled to costs and attorneys' fees.

1

Introduction

This chapter describes the commands used by the RFS7000 Series *Command Line Interface* (CLI). Access the CLI by running a terminal emulation program on a computer connected to the serial port at the front of the switch, or by using secure shell (ssh) to access the switch over the network.

1.1 Common Criteria Operational Requirements

To run the product in the Common Criteria evaluated configuration, the following conditions must be met:

1. The product shall run in the Common Criteria mode of operation. For configuration information please refer to the "Secure Installation Procedure" section of the *RFS7000GR Series RF Switch Installation Guide*
2. The product shall be configured to use an external FIPS-compliant RADIUS server for authentication of wireless users using EAP-TLS, EAP-PEAP or EAP-TTLS protocol.
3. The product shall use the internal administrator database for authentication of administrators
4. The product shall be configured to use an external NTP server for time synchronization
5. The product shall be configured to use an external audit server for transmission of audit records
6. Connections to the external servers shall be protected by an encrypted IPSec/IKE tunnel.
7. In support of the audit server, the IT environment shall provide the capability to protect audit information and authentication credentials. The environment shall also provide the capability to selectively view audit data.
8. In support of the authentication server, the IT environment shall provide facilities to manage authentication information and limit brute force password attacks.
9. Common Criteria Filter shall be enabled. Refer to *country-code on page 5-22* for details on the common-criteria command.

1.1.1 Configuration of MAC ACL For Common Criteria Operation

To run the product in the Common Criteria evaluated configuration, the following assumptions shall be satisfied:If

Table 1.1 Common Criteria Assumptions

Name	Assumption
A.NO_EVIL	Administrators shall be non-hostile, appropriately trained and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There shall be no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the product and the data it contains shall be provided by the environment.
A.TOE_NO_BYPASS	Wireless clients shall be configured so that information cannot flow between a wireless client and any other wireless client or host networked to the product without passing through the product.

access points are connected over L2 network then user shall use MAC ACLs as explained below.

```
RFS7000#
RFS7000#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RFS7000(config)#
```

Assigning IP Address to Management VLAN

```
RFS7000(config)#interface vlan 1
RFS7000(config-if)#ip address 172.17.1.100/24 RFS7000(config-if)#exit
```

Assiging access VLAN2 on GE1

```
RFS7000(config)#interface ge 1
RFS7000(config-if)#switchport mode access
RFS7000(config-if)#switchport access vlan 2
RFS7000(config-if)#exit
```

Assigning access VLAN3 on GE2

```
RFS7000(config)#interface ge 2
RFS7000(config-if)#switchport access mode access
RFS7000(config-if)#switchport access vlan 3
RFS7000(config-if)#exit
```

Assigning access VLAN4 on GE3

```
RFS7000(config)#interface ge 3
RFS7000(config-if)#switchport mode access
RFS7000(config-if)#switchport access vlan 4
RFS7000(config-if)#exit
```

Assigning management VLAN1 and VLAN20 (Data VLAN for WLAN 1) on GE4 TRUNK port.

```
RFS7000(config)#interface ge 4
RFS7000(config-if)#switchport mode trunk
RFS7000(config-if)#switchport trunk allowed vlan none
RFS7000(config-if)#switchport trunk allowed vlan add 1,20
RFS7000(config-if)#exit
```

Creating Data VLAN20 to use for WLAN1

```
RFS7000(config)#iinterface vlan 20
RFS7000(config-if)#ip address 172.2.1.100/24
RFS7000(config-if)#exit
```

Creating DHCP Server Pool to IP Addresses on VLAN20

```
RFS7000(config)#ip dhcp pool vlan20pool
RFS7000(config-dhcp)#address range 172.17.2.150 172.2.1.160
RFS7000(config-dhcp)#network 172.2.1.0/24
RFS7000(config-dhcp)#default-router 172.2.1.100
RFS7000(config-dhcp)#exit
RFS7000(config)#service dhcp
```

Creating WLAN1 with Preshared Key and Assiging VLAN20

```
RFS7000(config)#wireless
RFS7000(config-wireless)#wlan 1 ssid cc
RFS7000(config-wireless)#wlan 1 enable
RFS7000(config-wireless)#wlan 1 vlan 20
RFS7000(config-wireless)#wlan 1 dot11i key 12345678901234567890123456789012345678
901234567890123456789012345
RFS7000(config-wireless)#exit
```

Creating MAC ACL to assign to a physical port to allow only WISP packets.

```
RFS7000(config)#mac access-list extended
RFS7000(config)#mac access-list extended drop_nonwisp
RFS7000(config-ext-macl)#show interfaces ge1
Interface ge1 is UP
  Hardware-type: Ethernet, Mode: Layer 2, Address: 00-15-70-38-08-43
  Index: 2001, Metric: 1, MTU: 1500,  Status-flags: <UP,BROADCAST,RUNNING,MULTIC
AST>
  Speed: Admin Auto, Operational 100M, Maximum 1G
  Duplex: Admin Auto, Operational Full
  Active-medium: Copper
  Switchport settings: access, access-vlan: 2
  IP-Address: unassigned, primary
    Input packets 70619, bytes 8387001, dropped 0,
    Received 51086 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0,
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 55731, bytes 22076360, dropped 0
    Sent 66 broadcasts, 33948 multicasts
    Output errors 0, collisions 0, late collisions 0,
    Excessive collisions 0

RFS7000(config-ext-macl)#permit any 00-15-70-38-08-4c/00-15-70-38-08-4c type wisp
RFS7000(config-ext-macl)#exit
```

Applying MAC ACL to physical port GE1 and Running Configuration after Config Changes

```
RFS7000(config)#interface ge 1
RFS7000(config-if)#mac access-group drop_nonwisp in
RFS7000(config-if)#
RFS7000(config)#show  running-config
!
! configuration of RFS7000 version 4.1.0.0-010GNDR
!
version 1.4
!
!
aaa authentication login default local

network-element-id 172.2.1.0/24
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username "admin" privilege  superuser
username "operator" password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
mac access-list extended drop_nonwisp
 permit any 00:15:70:38:08:4c/00:15:70:38:08:4c type wisp rule-precedence 10
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
```

```
ip domain-name motorola.com
country-code us
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b45673a4fa870
snmp-server sysname RFS7000
snmp-server manager v3
snmp-server enable traps
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp authenticationFail
snmp-server enable traps diagnostics cpuLoad1Min
snmp-server enable traps diagnostics cpuLoad5Min
snmp-server enable traps diagnostics cpuLoad15Min
snmp-server enable traps wireless station associated
snmp-server enable traps wireless station disassociated
snmp-server enable traps wireless station deniedAssociationOnCapability
snmp-server enable traps wireless station deniedAssociationOnShortPream
snmp-server enable traps wireless station deniedAssociationOnSpectrum
snmp-server enable traps wireless station deniedAssociationOnErr
snmp-server enable traps wireless station deniedAssociationOnSSID
snmp-server enable traps wireless station deniedAssociationOnRates
snmp-server enable traps wireless station deniedAssociationOnInvalidWPAWPA2IE
snmp-server enable traps wireless station deniedAssociationAsPortCapacityReached
snmp-server enable traps wireless station deniedAuthentication
snmp-server enable traps wireless station radiusAuthFailed
snmp-server enable traps wireless station vlanChanged
snmp-server enable traps wireless radio adopted
snmp-server enable traps wireless radio unadopted
snmp-server enable traps wireless radio detectedRadar
snmp-server enable traps wireless ap-detection unauthorizedAPDetected
snmp-server enable traps wireless ap-detection unauthorizedAPRemoved
snmp-server enable traps wireless ids muExcessiveEvents
snmp-server enable traps wireless ids radioExcessiveEvents
snmp-server enable traps wireless ids switchExcessiveEvents
snmp-server enable traps mobility operationallyUp
snmp-server enable traps mobility operationallyDown
snmp-server enable traps mobility peerUp
snmp-server enable traps mobility peerDown
snmp-server enable traps wireless-statistics min-packets 10
snmp-server enable traps wireless-statistics wlan pktsps-greater-than 10.00
snmp-server enable traps wireless-statistics min-packets 10
firewall dhcp-snoop-conflict-detection disable
firewall dhcp-snoop-conflict-logging disable
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
no service pm sys-restart
!
wireless
 wlan 1 enable
 wlan 1 ssid cc
 wlan 1 vlan 20
 no ap-ip default-ap switch-ip
 smart-rf
 wireless
 !
!
radius-server local
 sole
!
interface ge1
 switchport access vlan 2
 ip dhcp trust
 mac access-group drop_nonwisp in
!
interface ge2
 switchport access vlan 3
 ip dhcp trust
!
interface ge3
 switchport access vlan 4
```

```
 ip dhcp trust
!
interface ge4
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 1,20,
 ip dhcp trust
!
interface me1
 ip address 10.1.1.100/24
!
interface vlan1
 ip address 172.17.1.100/24
!
interface vlan10
no ip address
!
interface vlan20
 ip address 172.2.1.100/24
!
ip dhcp pool vlan20pool
 address range 172.17.2.150
 address range 172.17.2.160
!
service dhcp
!
line con 0
line vty 0 24
!
auth-time 1
end

RFS7000(config-if)#
```

1.1.2 Configuration of IP ACL For Common Criteria Operation

If access points are connected over L3 network then user shall use MAC and IP ACLs in combination as explained below.

```
RFS7000#
RFS7000#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RFS7000(config)#
```

Assigning IP Address to Management VLAN

```
RFS7000(config)#interface vlan 1
RFS7000(config-if)#ip address 172.17.1.100/24
RFS7000(config-if)#exit
```

Assiging access VLAN2 on GE1

```
RFS7000(config)#interface ge 1
RFS7000(config-if)#switchport mode access
RFS7000(config-if)#switchport access vlan 20
RFS7000(config-if)#exit
```

Assiging management VLAN1 and VLAN20(Data VLAN for WLAN 1) on GE4 TRUNK port.

```
RFS7000(config)#interface ge 4
RFS7000(config-if)#switchport mode trunk
RFS7000(config-if)#switchport trunk allowed vlan none
RFS7000(config-if)#switchport trunk allowed vlan add 1,20
RFS7000(config-if)#exit
```

Creating Data VLAN20 to use for WLAN1

```
RFS7000(config)#iinterface vlan 20
RFS7000(config-if)#ip address 172.2.1.100/24
```

```
RFS7000(config-if)#exit
```

Creating DHCP Server Pool to IP Addresses on VLAN20

```
RFS7000(config)#ip dhcp pool vlan20pool
RFS7000(config-dhcp)#address range 172.17.2.150 172.2.1.160
RFS7000(config-dhcp)#network 172.2.1.0/24
RFS7000(config-dhcp)#default-router 172.2.1.100
RFS7000(config-dhcp)#exit
RFS7000(config)#service dhcp
```

Create ACL to block Non Capwap Packets(Allow only CAPWAP packets coming on UDP port 24576 and DHCP Port 67)

```
RFS7000(config)#ip access-list extended drop_noncapwap
RFS7000(config-ext-nacl)#permit udp host 172.16.1.99 host 172.2.1.100 eq 24576
RFS7000(config-ext-nacl)#permit udp host 0.0.0.0 host 255.255.255.255 eq 67 rule-
precedence 20
RFS7000(config-ext-nacl)#exit
RFS7000(config)#interface vlan 20
RFS7000(config-if)#ip access-group drop_noncapwap in
RFS7000(config-if)#exit
```

Creating MAC ACL to assign to a physical port to allow arp,ip and wisp packets.

```
RFS7000(config)#mac access-list extended drop_nonwisp
RFS7000(config-ext-macl)#permit any any type arp rule-precedence 5
RFS7000(config-ext-macl)#permit any any type ip rule-precedence 10
RFS7000(config-ext-macl)#permit any 00:15:70:13:f0:5e/00:15:70:13:f0:5e type wisp rule-
precedence 20
RFS7000(config-ext-macl)#exit
RFS7000(config)#interface ge 1
RFS7000(config-if)#mac access-group drop_nonwisp in
RFS7000(config-if)#exit
```

Creating WLAN1 with Preshared Key and Assiging VLAN20

```
RFS7000(config)#wireless
RFS7000(config-wireless)#wlan 1 ssid cc
RFS7000(config-wireless)#wlan 1 enable
RFS7000(config-wireless)#wlan1 1 vlan 20
RFS7000(config-wireless)#wlan 1 dot11i key 12345678901234567890123456789012345678
890123456789012345678901234
RFS7000(config-wireless)#exit
Adopt an AP300 to the switch over L2. (Connect a cable from GE1 to POE Switch and
conenct AP300 to POE Switch)and see AP300 is adopted to the switch.
RFS7000(config-wireless)#show wireless ap
Number of access-ports adopted   : 1
Available licenses               : 47
Redundancy enabled               : N
Redundancy mode                  : active
  # Mac Radios [indices]    Model-Number Adoption-Mode        Static IP
  1  00-A0-F8-D8-7E-94    2 [ 1 2 ]        WSAP-5110-100-WW L2 (vlan: 20)
RFS7000(config-wireless)#
Configure Static and Switch IP Addresses to AP 1
RFS7000(config-wireless)#ap-ip 1 ?
  static-ip  Static IP address, netmask and gateway address
  switch-ip  static switch IP addresses

RFS7000(config-wireless)#ap-ip 1 static-ip 172.16.1.99/24 172.16.1.101
RFS7000(config-wireless)#ap-ip 1 switch-ip add 172.2.1.100
RFS7000(config)#show wireless ap
Number of access-ports adopted   : 0
Number of AAPs adopted           : 0
Available AP licenses            : 0
Available AAP licenses           : 0
Redundancy enabled               : N
Redundancy mode                  : active


RFS7000(config)#
RFS7000(config)#
```

1.2 CLI Overview

The CLI is used for configuring, monitoring, and maintaining Motorola Solutions devices. The CLI interface allows you to execute commands, whether using a serial console or using remote access methods.

This chapter describes the basic features of the Motorola Solutions CLI and how to use them. Topics covered include an introduction to command modes, navigation and editing features, help features, and command history features.

The CLI is divided into different command modes. Each command mode has its own set of commands available for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in. Enter a question mark (**?**) at the system prompt to view the list of commands available for each command mode/ instance.

Use specific commands to navigate from one command mode to another. The standard order is as follows: USER EXEC mode; PRIV EXEC mode and GLOBAL CONFIG mode.

A session generally begins in USER EXEC mode, which is one of the two access levels of EXEC mode. For security purposes, only limited subset of EXEC commands are made available in USER EXEC mode. This level of access is reserved for tasks that do not change the configuration of the switch, such as determining the current switch configuration.

To access commands, enter the PRIV EXEC mode, which is the second level of access for the EXEC mode. In the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

Most of the USER EXEC mode commands are one-time commands and are not saved across reboots of the switch. For example, show command displays the current configuration and clear command clears the counter or interface.

Enter GLOBAL CONFIG mode from PRIV EXEC mode. In this mode, enter commands that configure general system characteristics. Use the global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allows you to make changes to the running configuration. If you save the configuration later, these commands are stored across switch reboots.

Enter a variety of protocol-specific or feature-specific configuration modes from global configuration mode. The CLI hierarchy requires you enter these specific configuration modes only through global configuration mode.

Enter configuration submodes from global configuration modes. Configuration submodes are used to configure specific features within the scope of a given configuration mode.

The *Table 1.2* summarizes the commands available to configure and monitor the switch.

Table 1.2 CLI Context Hierarchy for RFS7000

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
clear	acknowledge	aaa
clrscr	archive	aap-wlan-acl
cluster-cli	cd	access-banner
disable	change-passwd	access-list
enable	clear	arp
exit	clock	audit-log-filter
help	clrscr	auth-timeout
logout	cluster-cli	autoinstall

Table 1.2 CLI Context Hierarchy for RFS7000

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
no	configure	boot
page	copy	bridge
ping	debug	clrscr
quit	delete	country-code
service	diff	crypto
show	dir	do
terminal	disable	end
traceroute	edit	errdisable
	enable	exit
	erase	firewall
	exit	help
	halt	hostname
	help	interface
	keytransfer	ip
	kill	license
	logout	line
	mkdir	local
	more	logging
	no	mac
	page	mac-address-table
	ping	mac-name
	pwd	management
	quit	network-element-id
	reload	no
	rename	ntp
	rmdir	prompt
	run	radius-server
	service	ratelimit
	show	redundancy

Table 1.2 CLI Context Hierarchy for RFS7000

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
	terminal	remote-login
	traceroute	role
	upgrade	rtls
	upgrade-abort	service
	write	show
		smtp-notification
		snmp-server
		spanning-tree
		timezone
		traffic-shape
		username
		virtual-ip
		vpn
		wireless
		wlan-acl
		zeroize

1.3 Getting Context Sensitive Help

Enter a question mark (**?**) at the system prompt to display a list of commands available for each command mode. Optionally obtain a list of the arguments and keywords available for any command using context-sensitive help.

Use any of the following commands to get help specific to a command mode, command name, keyword or argument:

Table 1.3 Getting Context Sensitive Help Commands

Command	***Description***
(prompt)# **help**	Displays a brief description of the help system.
(prompt)# abbreviated-command-entry **?**	Lists commands in the current mode that begin with a particular character string.
(prompt)# abbreviated-command-entry **<Tab>**	Completes a partial command name.
(prompt)# **?**	Lists all commands available in the command mode.
prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command.

Table 1.3 Getting Context Sensitive Help Commands

Command	***Description***
(prompt)# command keyword ?	Lists the next available syntax option for the command.

NOTE The system prompt ma varies depending on which configuration mode you are in.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed by the question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word.

```
RFS7000#service?
  service  Service Commands

RFS7000#service
```

Enter a question mark (?) in place of a keyword or argument to list keywords or arguments. Include a space before the **?**. This form of help is called **command syntax help** and shows which keywords or arguments are available based on the command/ keywords and arguments already entered.

```
RFS7000>service ?
  clear        Reset functions
  diag         Diagnostics
  diag-shell   Provide diag shell access
  encrypt      Encrypt password or key with secret
  ip           Internet Protocol (IP)
  locator      flash all LEDS to locate switch visually
  pm           Process Monitor
  save-cli     Save CLI tree for all modes in html format
  securitymgr  Securitymgr parameters
  show         Show running system information
  smart-rf     Smart-RF Management Commands
  watchdog     enable the watchdog
  wireless     Wireless parameters


RFS7000>service
```

It is possible to abbreviate commands and keywords allowing a unique abbreviation. For example, configure terminal can be abbreviated as `config t`. Since the abbreviated form of the command is unique, the switch accepts the abbreviated form and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
RFS7000>help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000>
```

1.4 Using the no and default forms of Commands

Almost every configuration command has a `no` form. In general, use the no form to disable a feature or function. Use the command without the no keyword to re enable a disabled feature or enable a feature disabled by default.

1.5 Setting the Administrator Inactivity Timeout

To help prevent unauthorized access to the swtich, the adminstrator account will timeout and log off after 3 minutes of inactivity. To change the inactivity timeout, from the global configuration context issue the following commands:

RFS7000(config)# line console 0
RFS7000(config)# exec-timeout <timeout>

The valid timeout range is between 1-35791 minutes

1.6 Basic Conventions

The following are conventions to keep in mind while working within the CLI:

- Always use **?** at the end of the command to view if there are any further sub modes that can be used. If so, type the first few alphabets of the submode and press the tab key. Continue using **?** until you reach the final sub-submode.
- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`.
- Commands can be entered in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

NOTE CLI commands starting with `#`, at the `RFS7000#` prompt, are ignored and are not executed. Any leading space before a CLI command is ignored in execution

1.7 Using CLI Editing Features and Shortcuts

A variety of shortcuts and editing features are available. The following sections describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Deleting Entries*
- *Re-displaying the Current Command Line*
- *Transposing Mistyped Characters*
- *Controlling Capitalization*

1.7.1 Moving the Cursor on the Command Line

Table 1.4 shows the key combinations or sequences to move the cursor on the command line to make corrections or changes. **Ctrl** indicates the Control key, which must be pressed simultaneously with its associated letter key. **Esc** indicates the Escape key, which must be pressed first, followed by its associated letter key. Keys are not case sensitive. Many letters used for CLI navigation and editing were chosen to provide an easy means of remembering their functions.

In *Table 1.4*, bolded characters inside the ***Function Summary*** column indicate the relationship between the letter used and the function.

Table 1.4 Key Combinations Used to Move Cursor

Keystrokes	***Function Summary***	***Function Details***
Left Arrow or **Ctrl-B**	Back character	Moves the cursor one character to the left. When you enter a command extending beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to scroll back to the system prompt and verify the beginning of the command entry, or press the Ctrl-A key combination.
Right Arrow or **Ctrl-F**	Forward character	Moves the cursor one character to the right.
Esc, B	Back word	Moves the cursor back one word.
Esc, F	Forward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.
Ctrl-E	End of line	Moves the cursor to the end of the command line.
Ctrl-d		Deletes current character.
Ctrl-U		Deletes text up to cursor.
Ctrl-K		Deletes from cursor to end of line.
Ctrl-P		Gets the prior command from history.
Ctrl-N		Gets the next command from history.
Esc-C		Converts the rest of word to uppercase.
Esc-L		Converts the rest of word to lowercase.
Esc-D		Deletes the remainder of word.
Ctrl-W		Deletes a word up to the cursor.
Ctrl-Z		Enters the command and retursn to the root prompt.
Ctrl-L		Refreshes the input line.

1.7.2 Completing a Partial Command Name

Enter the first few letters of the command and press the **Tab** key if you do not remember the complete command name, or to reduce the amount of typing. The command line parser completes the command if the string entered is unique to the command mode. Use **Ctrl-I** if your keyboard does not have a Tab key.

The CLI recognizes a command once you have entered enough characters to make the command unique. For example, if you enter conf in privileged EXEC mode, the CLI associates your entry with the configure command only because the configure command begins with `conf`.

In the following example, the CLI recognizes the unique string for privileged EXEC mode of conf when the Tab key is pressed:

```
RFS7000# conf<Tab>
```

```
RFS7000# configure
```

When you use the command completion feature, the CLI displays the full command name. The command is not executed until you use the **Return** or **Enter** key. This way, the command can be modified if the full command was not what you intended by abbreviation. Enter a set of characters that could indicate more than one command to list commands that begin with that set of characters.

Alternatively, enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter you enter and the question mark (?).

For example, entering `co?` lists commands available in the current command mode:

```
RFS7000#co?
configure  Enter configuration mode
copy       Copy from one file to another

RFS7000#co
```

NOTE The characters entered before the question mark are reprinted to the screen to complete the command entry.

1.7.3 Deleting Entries

Use any of the following keystrokes to delete command entries:

Table 1.5 Keystrokes Used to Delete Command Entries

Keystrokes	*Purpose*
Backspace	Deletes the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-W	Deletes the word up to the cursor.
Esc, D	Deletes from the cursor to the end of the word.

1.7.4 Re-displaying the Current Command Line

It is easy to recall the current command line entry if the system suddenly displays a message when entering a command. To redisplay the current command line (refresh the screen), use the following keystroke:

Table 1.6 Keystrokes Used to Re-display Current Command

Keystrokes	*Purpose*
Ctrl-L	Redisplays the current command line.

1.7.5 Command Output pagination

When working with the CLI, output often extends beyond the visible screen length. In such a case, `Press Any Key to Continue (Q to Quit)` displays at the bottom of the screen. To resume, press the **Return** key to scroll down one line, or press the **Spacebar** to display the next full screen of output.

1.7.6 Transposing Mistyped Characters

If you have mistyped a command, it is possible to transpose the mistyped characters. To transpose characters, use the following keystroke:

Table 1.7 Keystrokes Used to Transpose Mistyped Characters

Keystrokes	Purpose
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

1.7.7 Controlling Capitalization

CLI commands are generally case-insensitive, and are typically in lowercase. To change the capitalization of the commands, use any of the following key sequences:

Table 1.8 Keystrokes Used to Change Captilization

Keystrokes	Purpose
Esc, C	Capitalizes the letters at the right of cursor.
Esc, L	Changes the letters at the right of cursor to lowercase.

2

Common Commands

This chapter describes the common CLI commands used in the USER EXEC and PRIV EXEC modes.

The PRIV EXEC command set contains the commands available in USER EXEC mode. Some commands can be entered in either mode. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If the user or privilege is not specified, the referenced command can be entered in either mode.

2.1 Common Commands

Table 2.1 summarizes commands common amongst many switch contexts and instances.

Table 2.1 Commands common in most contexts

Command	Description	Ref.
clrscr	Clears the display screen	*page 2-2*
exit	Ends the current mode and moves to the previous mode	*page 2-3*
help	Describes the interactive help system	*page 2-4*
no	Negates a command or set defaults	*page 2-6*
service	Displays service commands	*page 2-8*
show	Shows running system information	*page 2-25*

2.1.1 clrscr

Common Commands

Use this command to clear the screen and refresh the prompt (**#**).

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000#clrscr
```

2.1.2 exit

Common Commands

Use this command to end the current mode and move to the previous mode.

Note This command exits the current session and closes the terminal window in the User Exec and Priv Exec modes,

---

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config)#exit
RFS7000#
```

2.1.3 help

Common Commands

Use this command to access the advanced help feature. Use "**?**" at the command prompt to access the help topic.

Two styles of help are provided:

1. Full help is available when ready to enter a command argument and describe each possible argument. There is a space between the command and ?, (for example 'show ?').
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input. There is no space between the command and ?, (for example, 'show ve?').

Syntax

```
help
```

or

```
?
```

Parameters

None

Example

```
RFS7000>show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  environment           show environmental information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  service-list          List of services
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
```

```
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000>

RFS7000>show autoinstall ?
  |  Output modifiers
  >  Output redirection
  >>  Output redirection appending
RFS7000>show autoinstall status
Autoinstall not initiated
RFS7000>
```

2.1.4 no

Common Commands

Use this command to negate a command or set its defaults.

Syntax

```
no
```

Parameters

None

Example (User Exec)

```
RFS7000>no ?
  cluster-cli  Cluster context
  mobile-unit  mobile-unit index
  page         Toggle paging
  service      Service Commands

RFS7000>no
```

Example (Priv Exec)

```
RFS7000#no ?
  cluster-cli  Cluster context
  debug        Debugging functions
  mobile-unit  mobile-unit index
  page         Toggle paging
  service      Service Commands

RFS7000#no
```

Example (Global Config)

```
RFS7000(config)#no ?
  aaa                 VPN AAA authentication settings
  aap-wlan-acl        Remove an ACL from WLAN for AAP
  access-banner       Reset Access Banner to Default string
  access-list         Configure access-lists
  arp                 Address Resolution Protocol (ARP)
  auth-timeout        Set the AUTH timeout
  autoinstall         autoinstall configuration command
  bridge              Bridge group commands
  country-code        Clear the currently configured country code. All
                      existing radio configuration will be erased
  crypto              encryption module
  errdisable          Error Disable
  firewall            Wireless firewall
  hostname            Reset system's network name to default
  interface           Delete a virtual interface
  ip                  Internet Protocol (IP)
  line                Configure a terminal line
  local               Local user authentication database for VPN
  logging             Modify message logging facilities
  mac                 MAC configuration
  mac-address-table   Configure MAC address table
  mac-name            Remove a configured MAC address Name
  management          sets properties of the management interface
  network-element-id  Reset system's network element ID to default
  ntp                 Configure NTP
  prompt              Reset system's prompt
  radius-server       RADIUS server configuration commands
  ratelimit           ratelimit
  redundancy          Configure redundancy group parameters
  role                Configure role parameters
  service             Service Commands
  smtp-notification   Modify SMTP-Notification parameters
  snmp-server         Modify SNMP engine parameters
  spanning-tree       Spanning tree
  timezone            Revert the timezone to default (UTC)
```

```
  traffic-shape       Traffic shaping
  username            Establish User Name Authentication
  virtual-ip          Virtual IP
  vpn                 vpn
  wlan-acl            Remove an ACL from WLAN

RFS7000(config)#no
```

Example (Others)

```
RFS7000(config)#no service advanced-vty
RFS7000(config)#

RFS7000(config)#no bridge 1 ageing-time
RFS7000(config)#

RFS7000(config)#no bridge multiple-spanning-tree enable bridge-forward
RFS7000(config)#
```

2.1.5 service

Common Commands

Use this command to service/debug the switch.

Syntax (User Exec)

```
service [diag|encrypt|locator|save-cli|show|wireless]

service diag [enable|identify|limit (options)|period <100-30000>]

service diag limit [buffer[128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k]<0-65535>|
  fan <1-3> low <1000-15000>|filesys (etc2|flash|var) <LINE>|
  inodes (etc2|flash|var) <LINE>|load (01|15|05)|maxFDs <0-32767>|
  pkbuffers <0-65535>|procRAM <0.0-100.0>|ram <0.0-25.0>|
  routecache <0-65535>|temperature <1-6> (critical|high|low) <0.0-250.0>]

service encrypt (secret)<2> LINE

service locator

service save-cli

service show [cli|command-history|diag|info|memory|nsm|process|
  reboot-history|rtls|startup-log|upgrade-history|watchdog]
service show diag [hardware|led-status|limits|period|stats|top]
service show nsm virtual-ip config
service show rtls [location-history|stats]
```

Parameters (User Exec Only)

service (diag)	
enable	Enables service diagnostics
identify	Identifies this switch by flashing the LEDs
limit [buffer|fan|filesys| inodes|load|maxFDs| pkbuffers|procRAM| ram|routecache| temperature]	Sets the following diagnostic limits: • buffer – Sets buffer usage warning limit • fan – Sets fan speed limit • filesys – Sets file system free space limit • inodes – Sets file system inode limit • load – Sets aggregate processor load limit • maxFDs – Sets the maximum number of file descriptors • pkbuffers – Sets the packet buffer head cache limit • procRAM – Sets the percent RAM used by a process • ram – Sets the percent free RAM • routecache – Sets the IP route cache usage limit • temperature – Sets the switch sensor temperature limit

limit [buffer] [128|128k|16k| 1k|256|2k|32|32k|4k|512| 64|64k|8k] <0-65535>	Sets the diagnostic limit submodes/commands. Configure the buffer usage warning limit. The warning limit can be set to one of the following sizes: • buffer – Sets the buffer usage warning limit. • 128 – Sets 128 byte buffer limit • 128k – Sets 128k byte buffer limit • 16k – Sets 16k byte buffer limit • 1k – Sets 1k byte buffer limit • 256 – Sets 256 byte buffer limit • 2k – Sets 2k byte buffer limit • 32 – Sets 32 byte buffer limit • 32k – Sets 32k byte buffer limit • 4k – Sets 4k byte buffer limit • 512 – Sets 512 byte buffer limit • 64 – Sets 64 byte buffer limit • 64k – Sets 64k byte buffer limit • 8k – Sets 8 byte buffer limit • <0-65535> – Sets buffer usage warning limit between 0-65535
limit [fan] <1-3> [low <1000-15000>]	Sets the fan speed limit. Configure the fan speed limit for all three fans or just one. • <1-3> – Specifies the fan number • low <1000-15000> – Sets the selected fan speed limit between 1000 - 15000
limit [filesys] [etc2|flash|var] <LINE>	Sets the file system freespace limit. Select the freespace limit for the following sub context: • etc2 • flash • ram • <LINE> – Sets the selected file system freespace limit as a percentage
limit [inodes] [etc2|flash|var] <LINE>	Sets the file system inode limit. Select the freespace limit for the following sub context: • etc2 • flash • ram • <LINE> – Sets the selected file system inode limit as a percentage
limit [load] [01|15|05]	Configures the aggregate processor load. Select from the following submodes: • 01 – Aggregates processor load during the previous minute • 15 – Aggregates processor load during the previous 15 minute • 05 – Aggregates processor load during the previous 5 minute

limit [maxFDs] <0-32767>	Configures the maximum number of file descriptors between 0 - 32767
limit [pkbuffers] <0-65535>	Configures the packet buffer cache limit between 0 - 65535
limit [procRAM] <0.0-100.0>	Sets the RAM space used by a process as a percentage of the total space. Set the RAM space between 0 - 100.0%.
limit [ram] <0.0-25.0>	Sets the free space for the RAM as a percent of the total space. Set the free space between 0.0 - 25.0%.
limit [routecache] <0-65535>	Sets the IP route cache usage. Set a value between 0 - 65553.
limit [temperature] <1-6> [critical|high|low] <0.0-250.0>	Sets the temperature limit of the switch temperature sensor. Configures as many as 6 temperature sensors • critical – Sets critical temperature limit between 0.0 - 250.0 • high – Sets high temperature limit between 0.0 - 250.0 • low – Sets low temperature limit between 0.0 - 250.0
service (encrypt)	
encrypt (secret) 2 <LINE>	Encrypts passwords with a secret phrase using SHA256-AES256 encryption • <LINE> – Enter the encryption passphrase.
service (locator)	
locator	Flashes all LEDs to locate the switch visually
service (save-cli)	
save-cli	Saves CLI tree for all modes in HTML format
service (show)	
show [cli| command-history| diag|info| memory| nsm|process| reboot-history|rtls startup-log| upgrade-history| watchdog]	Displays following running system information: • cli – CLI tree of current mode • command-history – Command (except show commands) history • diag – System diagnostics • info – Available support information snapshot • memory – Memory statistics • nsm – *Network Services Manager* (NSM) configuration • process – Processes (sorted by memory usage) • reboot-history – Reboot history • rtls – *Real Time Locating System* (RTLS) statistics • startup-log – Startup log • upgrade-history – Upgrade history • watchdog – Watchdog status

show [diag] [hardware|led-status|limts|period|stats|top]	Shows following diagnostic details: • hardware – System hardware configuration • led-status – LED state variables and current state • limits – Limit values • period – The period (ms) for the in service diagnostics • stats – Current diagnostics statistics • top – Top processes (sorted by memory usage)
show [nsm] [virtual-ip] [config]	Shows the NSM virtual IP configuration
show [rtls] [location-history|stats]	Shows following RTLS statistics: • location-history – Location engine history • stats – *Smart Opportunistic Location Engine (*SOLE) algorithm statistics

Syntax (Priv Exec)

```
service [clear|diag|diag-shell|encrypt|firewall|ip|locator|
  password-encryption|pm|save-cli|securitymgr|show|smart-rf|start-shell|
  watchdog|wireless]

service clear [all|aplogs|clitree|fw (flows)|
  securitymgr (flows)[<0-349>|<WORD>|all|ge|me1|sa|vlan]|snooptable|
  wireless (mobile-unit) association-statistics]

service diag [enable|identify|limit|period]
service diag limit [buffer (128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k)
  <0-65535>|fan <1-3> (low) <1000-15000>|filesys (etc2|flash|var) <LINE>|
  inodes (etc2|flash|var) LINE|load (01|15|05) <0.0-100.0>|maxFDs <0-32767>|
  pkbuffers <0-65535>|procRAM <0.0-100.0>|ram <0.0-25.0>|
  routecache <0-65535>|temperature <1-6> (critical|high|low) <0.0-250.0>]

service diag-shell

service encrypt (secret)<2> LINE

service firewall (disable)

service ip (igmp) snooping robustness-variable <1-7>

service locator

service password-encryption (secret)<2> LINE

service pm (stop)

service save-cli

service securitymgr [disable|disable-flow-rate-limit]
```

```
service show [cli|command-history|diag|fw (flows) brief|info|memory|nsm|
  pm(history)[process-name|all]|process|radio-neighbor|reboot-history|rtls|
  securitymgr|smart-rf|startup-log|upgrade-history|watchdog|wireless]
service show diag [hardware|led-status|limits|period|stats|top]
service show ip (igmp) snooping [robustness-variable|vlan (<1-4094>|<VLAN>)]
service show radio-neighbor mu <MAC>
service show rtls [grid (all|x)|location-history|stats]
service show securitymgr flows (details|source)
service show smart-rf [debug-config|sensitivity (mu|pattern|rates)]

service show wireless [ap-history <MAC>|buffer-counters|
  enhanced-beacon-table (config|report)|enhanced-probe-table (config|report)|
  group <1-256>|group-stats|legacy-load-balance|mu-cache-buckets|
  mu-cache-entry (<1-8192>|<WORD>)|mvlan <1-256>|
  radio (<1-4094>|description|mapping>)|radio-cache-entry <WORD>|
  radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|
  vlan-cache-entry (<1-8192>|<WORD>)|waiting <0-99>]

service wireless [ap-history (clear|enable)|clear-ap-log <1-1024>|
  custom-cli|dot11i|enhanced-beacon-table|enhanced-probe-table|
  forward-eap-to-wired|free-packet-watermark <0-100>|
  idle-radio-send-multicast (enable)|legacy-load-balance|map-radios <1-127>|
  radio-misc-cfg <LINE>|rate-scale|request-ap-log <1-1024>|
  save-ap-log|snmp-trap-throttle <1-20>|sync-radio-entries|vlan-cache (enable)]

service wireless custom-cli [sh-wi-mobile-unit|sh-wi-radio]
service wireless dot11i (enforce) pmkid-validation
service wireless enhanced-beacon-table [channel-set|enable|erase-report|max-ap|
  scan-interval|scan-time]
service wireless enhanced-probe-table [enable|erase-report|max-mu|preferred|window-time]
```

Parameters (Priv Exec mode only)

service (clear)	
all	Clears all core, dump and panic files
aplogs	Clears all local AP log files (does not clear them off the AP)
clitree	Clears clitree.html file (created by the `save-cli` command)
fw [flows]	Clears established session flow details
securitymgr [flows] [<0-349>|<WORD>| all|ge|me1|sa|vlan]|	Clears the securitymgr flows based on the option selected. • <0-349> – Clears a specified flow. Specify the flow index between 1 - 349. • <WORD> – Clears flows for a specified interface. Specify the interface name. • all – Clears all established sessions • ge <1-4> – Clears GigabitEthernet interface flows. Specify the interface index between 1 - 4. • me1 – Clears FastEthernet interface flows. • sa <1-4> – Clears StaticAggregate interface flows. Specify the interface index between 1 - 4. • vlan <1-4094> – Clears VLAN interface flows. Specify the interface ID between 1 - 4094.
snooptable	Clears static and dynamic snoop entries
wireless [mobile-unit]	Clears *mobile unit* (MU) related parameters • association-statistics – Clears MU related association and reassociation statistics
service (diag)	
enable	Enables service diagnostics
identify	Identifies this switch by flashing the LEDs

limit [buffer|fan| filesys| inodes| load|maxFDs| pkbuffers| procRAM|ram| routecache| temperature]	Enables diagnostic limit commands
	• buffer [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k] <0-65535> – Sets buffer usage warning limits
	• fan <1-3> low <1000-15000> – Sets the fan speed limit of the fan specified by the <1-3> parameter
	  • <1000-1500> – Sets the fan speed limit between 1000 - 15000
	• filesys (etc2|flash|var) <LINE> – Sets the file system freespace limit for the selected sub context
	  • <LINE> – Sets the selected file system freespace limit as a percentage
	• inodes (etc2|flash|var) <LINE> – Sets the file system inode limit
	  • <LINE> – Sets the selected file system inode limit as a percentage
	• load (01|15|05) – Sets the aggregate processor load during the previous minutes, based on the option selected. The options are:
	  • 01 – Aggregates processor load during the previous minute
	  • 15 – Aggregates processor load during the previous 15 minutes
	  • 05 – Aggregates processor load during the previous 5 minutes
	• maxFDs <0-32767> – Configures the maximum number of file descriptors. Set the maximum number of file descriptors between 0 - 32767
	• pkbuffers <0-65535> – Configures the packet buffer cache limit. Set the buffer cache limit between 0 - 65535.
	• procRAM <0.0-100.0> – Sets the RAM space used by a process as a percentage of the total space. Set the RAM space between 0 - 100.0 percent.
	• ram <0.0-25.0> – Sets the free space for the RAM as a percent of the total space. Set the free space between 0.0 - 25.0 percent.
	• routecache <0-65535> – Defines the IP route cache usage between 0 - 65553
	• temperature <1-6> (critical|high|low) <0.0-250.0> – Sets the temperature limit of the switch temperature sensor. Sets as many as 6 temperature sensors
	  • critical <0.0-250.0> – Sets critical temperature limit between 0.0 - 250.0
	  • high <0.0-250.0> – Sets high temperature limit between 0.0 - 250.0
	  • low <0.0-250.0> – Sets low temperature limit between 0.0 - 250.0

period <100-30000>	Sets diagnostics period between 100 - 30000 milliseconds. The default period is 1000 milliseconds.
service (diag-shell)	
diag-shell	Provides diag shell access

service (encrypt)	
encrypt [secret] 2 <LINE>	Encrypts passwords with secret phrase, using SHA256-AES256 encryption • <LINE> – Enter the encryption passphrase.
service (firewall)	
firewall [disable]	Disables firewall parameters
service (ip)	
ip [igmp] [snooping] [robustness-variable <1-7>]	Sets *Internet Group Management Protocol* (IGMP) snooping parameters. • robustness-variable <1-7> – Sets the robustness count variable between 1 - 7
service (locator)	
locator	Flashes all LEDS to locate switch visually
service (pm)	
pm (stop)	Stops the *Process Monitor* (PM) from monitoring all daemons
service (save-cli)	
save-cli	Saves the CLI tree for all modes in the HTML format
service (securitymgr)	
securitymgr [disable|disable-flow-rate-limit]	Sets following securitymgr parameters: • disable – Disables the security manager • disable-flow-rate-limit – Disables flow rate limiting

service (show)	

show
[cli|
command-history|
diag|fw|
info|ip|
memory|nsm|
pm|
process|
radio-neighbor|
reboot-history|rtls|
securitymgr|smart-rf|
startup-log|
upgrade-history|
watchdog|
wireless]
	Displays the following running system information:
	• cli – Displays CLI tree of the current mode
	• command-history – Displays command (except show commands) history.diag – Displays following diagnostic parameters:
	  • hardware – System hardware configuration
	  • led-status – LED state variables and current state
	  • limits – Limit values
	  • period – The period (ms) for the in service diagnostics
	  • stats – Current diagnostics statistics
	  • top – Top processes (sorted by memory usage)
	• fw (flows) – Shows firewall flows
	  • flows (brief) – Shows brief summary of active flows
	• info – Displays available support information snapshot
	• ip [igmp] [snooping] –Displays IGMP snooping parameters
	  • robustness-variables – The robustness variable count
	  • vlan [<1-4094>|<VLAN>] – Identifies the VLAN(s) to use
	• memory – Shows memory statistics
	• nsm [variable-ip] [config] – Shows NSM configuration details
	• pm [history] [process-name|all] – Displays PM lite configuration parameters . The history log file has a time stamped single line for every deamon that is had been started/restarted.
	• process – Displays processes (sorted by memory usage)
	• radio-neighbor mu <MAC> – Shows the neighboring radios for a station
	  • mu <MAC> – Specify the MAC address of the *mobile unit* (MU) in the AA-BB-CC-DD-EE-FF format.
	• reboot-history – Displays reboot history
	• rtls [grid (all|x)|location-history|stats] – Shows following RTLS locating settings:
	  • grid (all|x) – RSSI values in grid. Shows all grids or the grid 'x' coordinate depending on the option selected
	  • location-history – Location engine history
	  • stats – SOLE statistics

	• securitymgr [flows] [details|source] – Displays following security manager flow details:
	  • details – Displays detail flow statistics
	  • source – Displays source IP address
	• startup-log – Displays start up log
	• upgrade-history – Displays upgrade history
	• watch – Displays watchdog status
	• wireless – Displays following wireless details:
	  • ap-history – Access port history
	  • buffer-counters – Allocation counts for various buffers
	  • enhanced-beacon-table – Enhanced beacon table for AP locationing
	  • enhanced-probe-table – Enhanced beacon table for MU locationing
	  • group – Radio group related debug information
	  • group-stats – Radio group statistics informationlegacy-load-balance – legacy load balance algorithm compatibility mode
	  • mu-cache-buckets – Wireless mobile units cache buckets
	  • mu-cache-entry – MU cache information (dumps whole table if no parameters given)
	  • mvlan – Multi-VLAN debug status
	  • radio – Radio serviceability parameters
	  • radio-cache-entry – Radio cache information (dumps whole table if no parameters given)
	  • radio-hash-buckets – Wireless radio hash buckets
	  • snmp-trap-throttle – Stats and parameters related to SNMP trap throttling
	  • vlan-cache-buckets – Wireless VLAN cache buckets
	  • vlan-cache-entry – MU VLAN cache information, dump whole table if no parameters given
	  • waiting – Waiting table contents

service (watchdog)	
watchdog	Enables the watchdog

service (wireless)	

wireless
[ap-history|
clear-ap-log <1-1024>|
custom-cli |dot11i|
enhanced-beacon-table|
enhanced-probe-table|
forward-eap-to-wired|
free-packet-watermark|
idle-radio-send-multicast|
legacy-load-balance|
map-radios <1-127>|
radio-misc-cfg|
rate-scale|
request-ap-log <11024>|
save-ap-log|
snmp-trap-throttle|
sync-radio-entries|vlan-cache]
	Configures Wireless parameters
	• ap-history (clear|enable) – Manages access port history
	  • clear – Clears all access port history
	  • enable – Enables AP history tracking
	• clear-ap-log <1-1024> – Clears AP flash logs
	  • <1-1024> – Select the flash index between 1-1024.
	• custom-cli [sh-wi-mobile-unit|sh-wi-radio] – Customizes the output of some summary CLI commands in wireless
	• dot11i (enforce) pmkid-validation – Modifies dot11i service parameters
	  • enforce (pmkid-validation) – Toggles PMKID validation in dot11i handshake message from client
	• enhanced-beacon-table – Sets enhanced beacon table parameters for AP locationing
	• enhanced-probe-table – Sets enhanced beacon table parameters for MU locationing
	• forward-eap-to-wired – Forwards EAP packets from a mobile unit to the wired side for the switch to perform 802.1x authentication. (Note: This does not apply for EAP frames directed to the BSS for wireless 802.1x authentication)
	• free-packet-watermark <0-100> – Sets the free packets threshold. If the percentage of free packets is lower than this number, then additional packets will not be queued up in the datapath.
	  • <0-100> – Sets the watermark percentage between 0 - 100
	• idle-radio-send-multicast (enable) – Enables forwarding of multicast packets to radios without associated mobile units
	• legacy-load-balance – Invokes legacy load balance algorithm with WS5100 3.0/3.0.1
	• map-radios <1-127> – Sets radio to CPU mapping constant between 1 - 127

	• radio-misc-cfg <LINE> – Sets radio-specific misc configuration U16 for all radios • <LINE> – The hexadecimal 0000-FFFF bit mask enabling/disabling various misc configurations • rate-scale – Enables wireless rate scaling (default) • request-ap-log <1-1024> – Requests AP logs. Set the AP index between 1 - 1024 • save-ap-log – Saves a debug/error sent by the access port • snmp-trap-throttle <1-20> – Limits the number of SNMP traps generated from the wireless table. Set the maximum number of traps to be generated per second between 1 - 20. • sync-radio-entries – Syncs radio configuration entries at cluster level • vlan-cache (enable) – Enables VLAN cache mode (default)
wireless (custom-cli) (sh-wi-mobile-unit)	Customizes the output of the "show wireless mobile unit" command. The options are: • ap-locn – Displays the location of the AP where this mobile unit is associated • ap-name – Name of the AP where the mobile unit is associated • channel – The channel of the radio where the mobile unit is associated • dot11-type – The dot11 radio type of the mobile unit • ip – The mobile unit's IP address • last-heard – The time when a packet was last received from the mobile unit • mac – The mobile unit's MAC address • radio-bss – The BSSID of the radio where the mobile unit is associated • radio-desc – The description of the radio where the mobile unit is associated • radio-id – The radio index to which the mobile unit is associated • ssid – The the mobile unit's WLAN SSID • state – The mobile unit's current state • vlan – The mobile unit's VLAN ID • wlan-desc – The WLAN description the mobile unit is using • wlan-id – The WLAN index the mobile unit is using

wireless (custom-cli) (sh-wi-radio)	Customizes the output of the "show radio" command. The options are: • adopt-info – Displays adoption information of the radio (whether its on current switch or on some other switch in a cluster) • ap-locn – Displays the location of the AP where the radio is associated • ap-mac – MAC address of the AP to which the radio belongs • channel – The configured and current channel of the radio • dot11-type – The dot11 type (11a/11g etc.) of the radio • num-mu – Number of mobile devices associated with this radio • power – The radio's configured and current power • pref-id – The radio's adoption preference ID • radio-bss – The radio's BSSID • radio-desc – The radio's description • radio-id – The radio index in configuration • state – The radio's current operational state

wireless
(enhanced-beacon-table)
	Sets following AP loactioning enhanced beacon table parameters:
	• channel-set [a|an|bg|bgn] – Adds channels to channel set for enhanced beacon table
	  • a <1-200> – Adds channels to channel-set for enhanced beacon table for 802.11a radios. List the channel number(s) between 1 - 200 (separate the channel numbers by space)
	  • an <1-200> – Adds channels to channel-set for enhanced beacon table for 802.11an radios. List the channel number(s) between 1 - 200 (separate the channel numbers by space)
	  • bg <1-200> – Adds channels to channel-set for enhanced beacon table for 802.11bg radios. List the channel number(s) between 1 - 200 (separate the channel numbers by space)
	  • bgn <1-200> – Adds channels to channel-set for enhanced beacon table for 802.11bgn radios.List the channel number(s) between 1 - 200 (separate the channel numbers by space)..
	• enable – Enables enhanced beacon table for AP locationing
	• erase-report – Erases the enhanced beacon table for AP locationing report
	• max-ap <0-512> – Sets the maximum number of APs in the enhanced beacon table for AP locationing. Set a number between 0 - 512.
	• scan-interval <10-60> – Sets the time duration between two enhanced beacon table for AP locationing scans in seconds. Set the time interval between 10 - 60 seconds.
	• scan-time <100-1000> – Sets the time duration of an enhanced beacon table in milliseconds. Set the duration between 100 - 1000 milliseconds.

wireless (enhanced-probe-table)	Sets the following MU loactioning enhanced beacon table parameters: • enable – Enables enhanced beacon table for MU locationing • erase-report – Erases the enhanced beacon table for MU locationing report • max-mu <0-512> – Sets the maximum number of MUs in the enhanced beacon table report. Set a number between 0 - 512. • preferred <MAC> – Adds the specified MAC address to the preferred MU list • window-time – Sets the window time for probe collection in seconds. Set the window time between 10 - 60 seconds.

Syntax (Global Config)

```
service [advanced-vty|dhcp|diag]

service diag [enable|limit|period]|pm(sys-restart)|radius (restart|test)|
  redundancy (dynamic-ap-load-balance) start|
  set [command-histroy|reboot-history|upgrade-history]|show (cli)|
  terminal-length <0-512>|watchdog]
```

Parameters(Global Config)

service (advanced-vty)	
advanced-vty	Enables advanced mode VTY interface
service (dhcp)	
dhcp	Enables the DHCP server service

service (diag)	
diag [enable|limit|period]	Use this parameter as a diagnostics tool. • enable – Enables in service diagnostics • limit – Sets diagnostic limits for following parameters: • buffer [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k] <0-65535> – Sets the buffer usage warning limit between 0 - 65535 • fan <1-3> low <1000-15000> – Sets the fan speed limit, of the selected fan, between 1000 - 15000 • filesys (etc2|flash|var) <LINE> – Sets the file system freespace limit, as a percent, for the selected file type • inodes (etc2|flash|var) <LINE> – Sets the file system inode limit, as a percent, for the selected file type • load (01|15|05) – Aggregates processor load during the previous minutes, based on the option selected • maxFDs <0-32767> – Sets the maximum number of file descriptors between 0 - 32767 • pkbuffers <0-65535> – Sets the packet buffer head cache between 0 - 65535 • procRAM <0.0-100.0> – Sets the RAM % used by a process between 0.0 - 100.0 • ram <0.0-25.0> – Sets the percent of free RAM between 0.0 - 25.0 • routecache <0-65535> – Sets the IP route cache usage limit between 0 -65535 • temperature <1-6> (critical|high|low) <0.0-250.0> – Sets the temperature limit for the switch temperature sensor. A maximum of six temperature sensors can be configured. • period <100-30000> – Sets diagnostics period between 100 - 30000 milliseconds. The default is 1000 milliseconds.
service (pm)	
pm (sys-restart)	Enables the *Process Monitor* (PM) • sys-restart – Enables PMLite to reboot the system when a deamon has been restarted maximum number of times. The default is to reboot the system. This enables the PM to restart the system when a process fails. **Note:** Use the `[no] service pm sys-restart` command to disallow a reboot of the system even after a process has been restarted to its maximum number of times. This is useful for debugging purpose.
service (radius)	

radius [restart|test]	Enables the RADIUS server. Select one of the following two options:
	• restart – Restarts the RADIUS server with updated configuration
	• test [<A.B.C.D>|<WORD>] – Tests the RADIUS server account with user parameters. Select the RADIUS server to test by providing one of the following information:
	  • <A.B.C.D> – The RADIUS server's IP address
	  • <WORD> – The RADIUS server's host name

service (set)	
set [command-history <10-300>| reboot-history <10-100>| upgrade-history <10-100>]	Sets service parameters • command-history <10-300> – Sets the size of the command history between 10 - 300. The default is 200. • reboot-history <10-100> – Sets the size of the reboot history between 0- 100. The default is 50. • upgrade-history <10-100> – Sets the size of the upgrade history between 10-100. The default is 50.
service (show)	
show [cli]	Displays running system information • cli – Displays the CLI tree of current mode
service (terminal-length)	
terminal-length [<0-512>]	Defines the system wide terminal length configuration • <0-512> – Sets the number of lines of VTY between 0 - 512 (0 means no line control)
service (watchdog)	
watchdog	Enables the watchdog

Example

```
RFS7000(config)#service diag ?
  enable  Enable in service diagnostics
  limit   diagnostic limit command
  period  Set diagnostics period


RFS7000#service diag limit ?
  buffer       buffer usage warning limit
  fan          Fan speed limit
  filesys      file system freespace limit
  inodes       file system inode limit
  load         agregate processor load
  maxFDs       maximum number of file descriptors
  pkbuffers    packet buffer head cache
  procRAM      percent RAM used by a process
  ram          percent free RAM
  routecache   IP route cache usage
  temperature  temperature limit


RFS7000(config)#service diag limit load ?
  01  during the previous minute
  05  during the previous 05 minutes
  15  during the previous 15 minutes
```

```
RFS7000#service diag limit load 05 ?
  WORD  percentage load from 0.0 to 100.0

RFS7000#service diag limit load 05 50

RFS7000#service diag limit maxFDs ?
  <0-32767>  0-32767

RFS7000#service diag limit maxFDs 30000

RFS7000#service diag limit pkbuffers ?
  <0-65535>  limit from 0-65535


RFS7000(config)#service terminal-length ?
  <0-512>  Number of lines of VTY (0 means no line control)


RFS7000(config)#service watchdog ?
```

2.1.6 show

Common Commands

This command displays the settings for the specified system component. There are a number of ways to invoke the show command:

- Invoked without any arguments, show displays information about the current context. If the current context contains instances, then show command (usually) displays a list of these instances.
- Invoked with the display parameter, it displays information about that component.

Syntax

```
show [display_parameter]
```

Parameters

Table 2.2 Show commands common to all modes

Display Parameters	Description	Mode	Example
aap-wlan-acl	Displays wlan based ACL	Common	*page 2-28*
aap-wlan-acl-stats	Displays IP filtering WLAN based statistics	Common	*page 2-29*
access-banner	Displays access banner	Common	*page 2-30*
audit-log-filters	Displays audit log filter rules	Common	*page 2-31*
autoinstall	Displays autoinstall configuration	Common	*page 2-32*
commands	Displays a command lists	Common	*page 2-33*
crypto	Displays encryption details	Common	*page 2-34*
crypto-error-log	Display crypto error logs	Common	*page 2-36*
crypto-log	Displays crypto log	Common	*page 2-37*
environment	Displays environmental information	Common	*page 2-38*
firewall	Displays Wireless firewalls		*page 2-39*
history	Displays the session command history	Common	*page 2-40*
interfaces	Displays interface status and configuration	Common	*page 2-41*
ip	Displays the *Internet Protocol* (IP)	Common	*page 2-43*
ldap	Displays LDAP server configuration	Common	*page 2-48*
licenses	Displays installed licenses, if any	Common	*page 2-49*
logging	Displays the log configuration and buffer	Common	*page 2-50*
mac	Displays the *media access control* (MAC)ACL configurations	Common	*page 2-51*
mac-address-table	Displays MAC address table	Common	*page 2-52*
mac-name	Displays the configured MAC names	Common	*page 2-53*

Table 2.2 Show commands common to all modes

Display Parameters	Description	Mode	Example
management	Displays the L3 management interface name	Common	*page 2-54*
mobility	Displays mobility parameters	Common	*page 2-55*
ntp	Displays *network time protocol* (NTP) settings	Common	*page 2-57*
port	Displays physical/aggregate port interface	Common	*page 2-58*
port-channel	Displays port channel commands	Common	*page 2-59*
privilege	Displays the current privilege level	Common	*page 2-60*
protocol-list	Displays list of protocols	Common	*page 2-61*
radius	Displays RADIUS configuration commands	Common	*page 2-62*
redundancy	Displays redundancy group parameters	Common	*page 2-63*
role	Displays role parameters	Common	*page 2-64*
rtls	Displays *Real Time Locating System* (RTLS) configuration	Common	*page 2-65*
service-list	Displays list of services	Common	*page 2-67*
smtp-notification	Displays SNMP engine parameters	Common	*page 2-68*
snmp	Displays SNMP engine parameters	Common	*page 2-69*
snmp-server	Display SNMP engine parameters	Common	*page 2-70*
spanning-tree	Displays spanning-tree information	Common	*page 2-71*
static-channel-group	Displays the contents of static channel group membership	Common	*page 2-73*
terminal	Displays terminal configuration parameters	Common	*page 2-74*
timezone	Displays the timezone	Common	*page 2-75*
traffic shape	Displays traffic shaping	Common	*page 2-76*
users	Displays terminal line information	Common	*page 2-77*
version	Displays software and hardware versions	Common	*page 2-78*
virtual ip	Displays IP redundancy feature	Common	*page 2-79*
wireless	Displays wireless configuration commands	Common	*page 2-80*
wlan-acl	Displays WLAN based ACL information	Common	*page 2-104*

Table 2.3 Show commands in PrivExec and Global Config modes

Display Parameters	Description	Mode	Example
access-list	Displays access list IP configuration	Privilege/Global Config	*page 2-91*
aclstats	Displays ACL statistics	Privilege/Global Config	*page 2-92*
boot	Displays the boot configuration	Privilege/Global Config	*page 2-93*
clock	Displays the system clock	Privilege/Global Config	*page 2-94*
debugging	Displays debug settings	Privilege/Global Config	*page 2-95*
dhcp	Displays DHCP server configuration	Privilege/Global Config	*page 2-96*
file	Displays filesystem information	Privilege/Global Config	*page 2-97*
password-encryption	Displays the password's encryption settings	Privilege/Global Config	*page 2-98*
running-config	Displays the current operating configuration	Privilege/Global Config	*page 2-99*
securitymgr	Displays debug info for ACL, VPN and NAT	Privilege/Global Config	*page 2-100*
sessions	Displays active open (current) connections	Privilege/Global Config	*page 2-68*
startup-config	Displays the contents of the startup configuration	Privilege/Global Config	*page 2-102*
upgrade-status	Displays last image upgrade status	Privilege/Global Config	page 2-103

2.1.7 aap-wlan-acl

Show commands common to all modes

Use this command to display WLAN based ACL.

Syntax

```
show aap-wlan-acl [<1-256>|all]
```

Parameters

<1-256>	Displays ACLs attached to the specified WLAN ID for AAP
all	Displays ACLs attached to WLAN port

Example

```
RFS7000#show aap-wlan-acl all
RFS7000#
```

2.1.8 aap-wlan-acl-stats

Show commands common to all modes

Use this command to display IP filtering WLAN based statistics.

Syntax

```
show aap-wlan-acl-stats
```

Parameters

None

Example

```
RFS7000#show aap-wlan-acl-stats
IP Filtering Statistics:
RFS7000#
```

2.1.9 access-banner

Show commands common to all modes

Use this command to display access banner.

Syntax

```
show access-banner
```

Parameters

None

Example

```
RFS7000(config)#show access-banner
This Device is running in Common Criteria Mode
Attention:
This is a protected and private wireless system. No un-authorized access allowed

You must have proper rights to access and manage this system from the authorized
 personnel.
RFS7000(config)#
```

2.1.10 audit-log-filters

Show commands common to all modes

Use this command to display audit log filter rules.

Syntax

```
show audit-log-filters
```

Parameters

None

Example

```
RFS7000#show audit-log-filters
  RULE-PRECEDENCE  USERNAME SOURCE    MAC-address IP-address ACTION
RFS7000#
```

2.1.11 autoinstall

Show commands common to all modes

Use this command to display autoinstall configuration.

Syntax

```
show autoinstall {status}
```

Parameters

status	Optional. Displays autoinstall status (whether initiated or not)

Example

```
RFS7000(config)#show autoinstall
Warning: This will display secure information.Do you want to proceed? (y/n): y
feature    enabled      URL
config       yes        --not-set--
cluster cfg  yes        --not-set--
image        yes        --not-set--
expected image version  --not-set--
RFS7000(config)#

RFS7000(config)#show autoinstall status
Autoinstall not initiated
RFS7000(config)#
```

2.1.12 commands

Show commands common to all modes

Use this command to view a list of show commands.

Syntax

```
RFS7000>show commands
```

Parameters

None

Example

```
RFS7000>show commands
  help
  show commands
  show ip http secure-server
  show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>'
  show ip access-group all
  show ip access-group role ( WORD | )
  show ip arp
  show ip ddns binding
  show ip dhcp binding
  show ip dhcp binding manual
  show ip dhcp class ( WORD | )
  show ip dhcp pool ( WORD | )
  show ip dhcp sharednetwork
  show ip dhcp-vendor-options
  show ip domain-name
  show ip interface (brief|)
  show ip interface (`WORD|vlan <1-4094>' (brief|)|)
  show ip name-server
  show ip route (detail|)
  show ip route A.B.C.D
  show ip route A.B.C.D/M
  show ip routing
  show ip ssh
  show rtls (aeroscout|ekahau|sole)
  show rtls sole peers
  show rtls sole probes (aeroscout|ekahau|mobile-unit|A<A-BB-CC-DD-EE-FF|)
  show rtls filter (<1-100>|)
  show rtls site
  show rtls tags (mobile-unit|rfid|aeroscout|ekahau|g2|) (all|)
  show rtls tags zone <1-48> (all|)
  show rtls zone (<1-48>|)
  show rtls zone (<1-48>|) detail
  show aap-wlan-acl (<1-256>)
  show aap-wlan-acl all
  show aap-wlan-acl-stats
  show audit-log-filters
  show autoinstall
  show autoinstall status
  show crypto ipsec sa
  show crypto ipsec security-association lifetime
  show crypto ipsec transformset ( WORD | )
  show crypto isakmp policy ( <1-10000> | )
  show crypto isakmp sa
  show crypto map (interface WORD | tag WORD |)
  show environment
  show firewall config
  show firewall dhcp snoop-table
  show firewall flow timeouts
  show interfaces (`WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>'|)
  show interfaces switchport `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>'
  show ldap configuration (primary|secondary|)
  show licenses
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000>
```

2.1.13 crypto

Show commands common to all modes

Use this command to display encryption module configuration.

Syntax

```
show crypto [ipsec|isakmp|key|map|pki]

show crypto ipsec(sa|security-association(lifetime)|transformset <NAME>)
show crypto isakmp(policy(<1-10000>)|sa)
show crypto key(mypubkey)(rsa)
show crypto map(interface <NAME>|tag <NAME>)
show crypto pki(request <NAME>|trustpoints)
```

Parameters

ipsec [sa| security-association [lifetime]| transformset {<NAME>}]	Displays following IPSec policy settings: • sa – IPSec *security associations* (SAs) • security-association [lifetime] – Lifetime IPSec SAs • transformset <NAME> – IPSec transformsets • <NAME> – Specify the transformset name.
isakmp [policy <1-10000>|sa]	Displays following *Internet Security Association and Key Management Protocol* (ISAKMP) policy settings: • policy <1-10000> – Priority all ISAKMP policies. • sa – All crypto ISAKMP SAs
key [mypubkey] [rsa]	Displays following authentication key management settings: • mypubkey [rsa] – Public keys associated with the switch • rsa – RSA public keys
map [interface|tag] <NAME>	Displays following crypto maps: • interface <NAME> – Crypto maps for a specified interface. Specify the interface name to display associated crypto map. • tag <NAME> – Crypto maps with a specified tag. Specify the crypto map tag to display. • <WORD> – The interface/tag name
pki [request <NAME>| trustpoints]	Displays following *Public Key Infrastructure* (PKI) settings: • request <NAME> – A specified certificate request. Specify the request name. • trustpoints – Configured trustpoint settings

Usage Guidelines

The security engine updates the IPSec and ISAKMP statistics every 60 seconds.

Example

```
RFS7000#show crypto pki trustpoints

Trustpoint :default-trustpoint
------------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:         Motorola
      Organizational Unit: EWLAN
      Organization:        Enterprise Mobility
      Location:            San Jose
      State:               CA
      Country:             US
    Issuer Name:
      Common Name:         Motorola
      Organizational Unit: EWLAN
      Organization:        Enterprise Mobility
      Location:            San Jose
      State:               CA
      Country:             US
  Valid From:   Aug 27 04:30:03 2011 GMT
  Valid Until:  Aug 26 04:30:03 2012 GMT

RFS7000#

RFS7000#show crypto key mypubkey rsa
Warning: This will display secure information.Do you want to proceed? (y/n): y

Key name: default_ssh_rsa_key
 Key length in bits: 2048
 Key Data
  BC0F487 8337B3C C042CB4 2281181 0DB5034 C31523D 3CD70B9 4489EF8
  C8664C9 C1A75BF 9B3ECEB 2E59B4D 13320B3 BF6EF37 A3D7273 5E5E76E
  25C5DE4 52441E4 155164A BAFDF11 95FA01A C807D1C 057496D 27F0558
  71711EA 405E1A4 20A8318 734B805 6A99634 9858C91 532BFB6 65D3A74
  197416B B4D0C89 930280D C2A7678 1FA65AC C403DDE 780F1C5 9C63C71
  A7A31F5 E07A255 313C109 B0B1700 EC01FF2 BE0A6FF A961408 369BC96
  D87A25A 3357E50 DB3440C 14DE17A F0C1F30 644DD7A 65DB8F7 6D7C72C
  D441C94 12A34A7 63729ED 690E9BE 0609E5B 0EF696B D7CAA39 91FEA26
  23

Key name: default_ssh_rsa_key.pub
RFS7000#

RFS7000(config)#show crypto ipsec security-association lifetime
Security-association lifetime: 204800 kilobytes / 3600 seconds
RFS7000(config)#

RFS7000(config)#show crypto ipsec sa ?
  |  Output modifiers
  >  Output redirection
  >>  Output redirection appending
  <cr>

RFS7000(config)#show crypto ipsec sa | ?
  append    Append output
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output

RFS7000(config)#show crypto ipsec sa | append ?
  FILE  Output file name

RFS7000(config)#show crypto ipsec sa | append FILE ?
  <cr>

RFS7000(config)#show crypto ipsec sa | append FILE
```

2.1.14 crypto-error-log

Show commands common to all modes

Use this command to display crypto error log.

Syntax

```
show crypto-error-log
```

Parameters

None

Example

```
RFS7000(config)#show crypto-error-log ?
  |  Output modifiers
  >  Output redirection
  >>  Output redirection appending
  <cr>

RFS7000(config)#show crypto-error-log | ?
  append    Append output
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output

RFS7000(config)#show crypto-error-log | append ?
  FILE  Output file name

RFS7000(config)#show crypto-error-log | append FILE ?
  <cr>

RFS7000(config)#show crypto-error-log | append FILE
RFS7000(config)#
```

2.1.15 crypto-log

Show commands common to all modes

Use this command to display crypto log.

Syntax

```
show crypto-log
```

Parameters

None

Example

```
RFS7000(config)#show crypto-log
FIPS Power-On Self Test started
Sat Aug 27 04:28:32 2011   FIPS self test started this can take some time
Sat Aug 27 04:28:32 2011   Creating integrity check file as a part of the update process
Sat Aug 27 04:29:49 2011   FIPS integrity check of the WIOS image successful
Sat Aug 27 04:29:49 2011   FIPS data integrity check is successful
Sat Aug 27 04:29:49 2011   FIPS power-up tests for openSSL library
Sat Aug 27 04:29:51 2011   1. Automatic power-up self test includes RNG, HMAC, AES,
3DES, RSA selftests...Successful
Sat Aug 27 04:29:51 2011   2. AES encryption/decryption...Successful
Sat Aug 27 04:29:52 2011   3. RSA key generation and encryption/decryption...successful
Sat Aug 27 04:29:52 2011   5a. SHA-1 hash...successful
Sat Aug 27 04:29:52 2011   5b. SHA-256 hash...successful
Sat Aug 27 04:29:52 2011   5c. SHA-512 hash...successful
Sat Aug 27 04:29:52 2011   5d. HMAC-SHA-1 hash...successful
Sat Aug 27 04:29:52 2011   5e. HMAC-SHA-224 hash...successful
Sat Aug 27 04:29:52 2011   5f. HMAC-SHA-256 hash...successful
Sat Aug 27 04:29:52 2011   5g. HMAC-SHA-384 hash...successful
Sat Aug 27 04:29:52 2011   5h. HMAC-SHA-512 hash...successful
Sat Aug 27 04:29:52 2011   The tests completed without errors
 ..............................................................................

RFS7000(config)#
```

2.1.16 environment

Show commands common to all modes

Use this command to display environmental information.

Syntax

```
show environment
```

Parameters

None

Example

```
RFS7000(config)#show environment
                    upwind of CPU temperature :  30.0 C
                          CPU die temperature :  56.0 C
                       left side temperature :  29.0 C
                         by FPGA temperature :  27.0 C
                      front right temperature :  25.0 C
                       front left temperature :  26.0 C
                            fan 1 fan         :  6540 rpm
                            fan 2 fan         :  6780 rpm
                            fan 3 fan         :  6600 rpm
RFS7000(config)#
```

2.1.17 firewall

Show commands common to all modes

Use this command to display firewall configuration.

Syntax

```
show firewall [config|dhcp (snoop-table)|flow (timeouts)]
```

Parameters

config	Displays firewall configuration
dhcp based [snoop-table]	Displays DHCP snoop table entries
flow [timeouts]	Displays flow timeout configuration

Example

```
RFS7000#show firewall config
Wireless firewall: enabled
  IPv4 virtual defragmentation: enabled
  IPv4 TCP MSS clamping: enabled
  IPv4 path-MTU clamping: disabled
  802.2 encapsulations: denied
  802.1q vlan stacking: denied
RFS7000#
```

2.1.18 history

Show commands common to all modes

Use this command to display session command history.

Syntax

```
show history
```

Parameters

None

Example

```
RRFS7000>show history
Warning: This will display secure information.Do you want to proceed? (y/n): y
   1 admin
   2 en
   3 disable
   4 en
   5 configure terminal
   6 show
   7 exit
   8 show audit-log-filters
   9 show commands
  10 disable
  11 show commands
  12 en
  13 show crypto ipsec security-association lifetime
  14 show crypto ipsec sa
  15 show crypto ipsec security-association lifetime
  16 show crypto ipsec transformset
  17 show crypto pki trustpoints
  18 show crypto key mypubkey rsa
  19 show crypto ipsec security-association lifetime
  20 show crypto ipsec sa
  21 show crypto ipsec sa | append FILE
  22 configure terminal

.....................................................................................
.
RFS7000>
```

2.1.19 interfaces

Show commands common to all modes

Use this command to display interface status.

Syntax

```
show interfaces {<IFNAME>|ge <1-4>|me1|sa <1-4>|
  switchport[<IFNAME>|ge <1-4>|me1|sa <1-4>|vlan <1-4094>]|vlan <1-4094>}
```

Parameters

<IFNAME>	Optional. Displays a specified interface status. Specify the interface name to display status.
ge <1-4>	Optional. Displays GigabitEthernet interface status. Select the interface index between 1- 4.
me1	Optional. Displays FastEthernet interface status
sa <1-4>	Optional.Displays StaticAggregate interface status. Select the interface index between 1 - 4.
switchport [<IFNAME>| ge <1-4>|me1| sa <1-4>|vlan <1-4094>]	Optional.Displays status of layer2 interfaces. Select from the following L2 interfaces: • <IFNAME> – Specify the switch interface name to display status. • ge <1-4> – Displays GigabitEthernet interface status. Select the interface index between 1 - 4. • me1 – Displays layer2 FastEthernet interface status. • sa <1-4> – Displays StaticAggregate interface status. Select the interface index between 1 - 4. • vlan – Displays layer2 VLAN interface status. Select the VLAN interface index between 1 - 4094.
vlan <1-4094>	Optional. Displays the VLAN interface status. Select an index value between 1- 4094.

Example

```
RFS7000(config)#show interfaces ge 1
Interface ge1 is UP
  Hardware-type: Ethernet, Mode: Layer 2, Address: 00-15-70-38-08-43
  Index: 2001, Metric: 1, MTU: 1500,  Status-flags: <UP,BROADCAST,RUNNING,MULTIC
AST>
  Speed: Admin Auto, Operational 100M, Maximum 1G
  Duplex: Admin Auto, Operational Full
  Active-medium: Copper
  Switchport settings: access, access-vlan: 10
  IP-Address: unassigned, primary
    Input packets 8900, bytes 887098, dropped 0,
    Received 6106 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0,
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 25504, bytes 3134441, dropped 0
    Sent 21 broadcasts, 23115 multicasts
    Output errors 0, collisions 0, late collisions 0,
    Excessive collisions 0
RFS7000(config)#
```

```
RFS7000(config)#show interfaces sa 2
Interface sa2
  Hardware Type AGGREGATE, Interface Mode Layer 2, address is 00-15-70-37-fc-91
  index=2005, metric=1, mtu=0, (HAL-IF)  <>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
RFS7000(config)#
```

2.1.20 ip

Show commands common to all modes

Use this command to view IP configuration details.

Syntax

```
show ip [access-group| access-list|arp|ddns|dhcp|dhcp-vendor-options|
  domain-name|dos|http|igmp|interface|name-server|nat|route|routing|ssh]

show ip access-group (<IFNAME>|all|ge <1-4>|me1|role <NAME>|sa <1-4>|vlan <1-4094>)

show ip access-list

show ip arp

show ip ddns [binding]

show ip dhcp [binding (manual)|class <NAME>|pool <NAME>|sharednetwork]

show ip dhcp-vendor-options

show ip domain-name

show ip dos [config|stats]

show ip http [secure-server]

show ip igmp snooping {mrouter|querier|vlan}

show ip interface {<IFNAME>|brief|vlan}

show ip name-server

show ip nat [interfaces|translations {inside [destination|source]|
  outside [destination|source]|verbose}]

show ip route {A.B.C.D|A.B.C.D/M|detail}

show ip routing

show ip ssh
```

Parameters

show ip (access-group)	
access-group [<IFNAME>|all| ge <1-4>|me1| role <NAME>| sa <1-4>|vlan <1-4094>]	Displays the ACLs attached to an interface. Select one of the following options to view ACL: • <IFNAME> - Displays ACLs attached to a specified interface. Specify the interface name. • all - Displays ACLs attached on all interfaces • ge - Displays ACLs attached to GigabitEthernet interface • me1 - Displays ACLs attached to FastEthernet interface • role - Displays ACLs attached to a specified role. Specify the role name. • sa - Displays ACLs attached to StaticAggregate interface • vlan - Displays ACLs attached to VLAN interface
show ip (access-list)	
access-list	Lists IP access lists

show ip (arp)	
arp	Displays *Address Resolution Protocol* (ARP) settings
show ip (ddns)	
ddns [binding]	Displays DNS address bindings
show ip (dhcp)	

dhcp [binding {manual}|
class {<NAME>}|
pool {<NAME>}|
sharednetwork]
	Displays following DHCP server configuration:
	• binding – DHCP address bindings
	  • manual – Optional. Static DHCP address bindings
	• class – Displays DHCP server class configuration
	  • <NAME> – Optional. Specify the class name, to view configuration.
	• pool – Displays DHCP pools.
	  • <NAME> – Optional. Specify the DHCP pool name, to view configuration.
	• sharednetwork – Displays shared networks

show ip (dhcp-vendor-options)	
dhcp-vendor-options	Displays DHCP Option 43 parameters received from DHCP server
show ip (domain-name)	
domain-name	Displays default domain for DNS
show ip (dos)	
dos (config|stats)	Displays following *Denial of Service* (DOS) configuration: • config – IP DOS configuration • stats – IP DOS statistics
show ip (http)	
http (secure-server)	Displays *Hyper Text Transfer Protocol* (HTTP) settings • secure-server – Secure HTTP server (HTTPS)
show ip (igmp)	
igmp (snooping) {mrouter|querier|vlan}	Displays *Internet Group Management Protocol* (IGMP) settings • snooping – Displays IGMP snooping settings

mrouter (vlan)
[<1-4094>|<VLAN-LIST>]
	Optional. Displays multicast router settings
	• vlan – Identifies the VLAN to use
	  • <1-4094> – Select a single VLAN index between 1 - 4094.
	  • <VLAN-LIST> – Specify a list (for example, 1,3,7) or range (for example, 3-7) of VLANs.

querier (vlan) [<1-4094>|<VLAN-LIST>]	Optional. Displays IGMP querier settings
	• vlan – Identifies the VLAN to use
	  • <1-4094> – Select a single VLAN between 1 - 4094.
	  • <VLAN-LIST> – Specify a list (for example, 1,3,7) or range (for example, 3-7) of VLANs.

valn [<1-4094>| <VLAN-LIST>]	Optional. Identifies the VLAN to use • <1-4094> – Select a single VLAN between 1 - 4094. • <VLAN-LIST> – Specify a list (for example, 1,3,7) or range (for example, 3-7) of VLANs.
show ip (interface)	
interface {<IFNAME> {brief}| brief| vlan <1-4094> {brief}}	Displays IP interface status and configuration based on the option selected. The options are: • <IFNAME> {brief} – Optional. Specify the interface name to view status and configuration. • brief – Optional. Displays brief summary of IP status and configuration of all interfaces • vlan <1-4094> {brief} – Optional. Displays VLAN interface IP status and configuration. Specify the VLAN interface ID between 1 - 4094. • brief – Optional. Displays a brief summary based on the option selected
show ip (name-server)	
name-server	Displays DNS name servers
show ip (nat)	
ip nat (interface) [interfaces|translations]	Displays following *Network Address Translation* (NAT) configuration:interfaces – Displays NAT configuration on Interfaces • translations – Displays NAT translations

ip nat (translations) {inside (destination|source)| outside (destination|source)| verbose}	Displays NAT translations.
	• inside – Optional. Inside
	  • destination – Destination
	  • source – Source
	• outside – Optional. Outside
	  • destination – Destination
	  • source – Source
	• verbose – Optional. NAT translations in real time

show ip (route)	

route {<A.B.C.D>|<A.B.C.D/M>|detail}	Displays IP routing table • A.B.C.D – Optional. Displays the network in the IP routing table • A.B.C.D/M – Optional. IP prefix <network>/<length> (for example, 35.0.0.0/8) • detail – Optional. Displays IP routing table in detail
show ip (routing)	
routing	Displays IP routing status
show ip (ssh)	
ssh	Displays *Secured Shell* (SSH) server details

Usage Guidelines

1. It has been noted the interface and VLAN status is displayed as UP despite of a disconnection. In such a case, shutdown the VLAN. Follow these steps:
   a. Check the status of the interface and VLAN:

```
RFS7000(config)#show ip interface brief
a. Interface            IP-Address/Mask         Status              Protocol
a. me1                  10.1.1.100/24           up                  down
a. vlan1                unassigned              up                  up
a. vlan10               172.16.10.1/24          up                  up
a. RFS7000(config)#
```

   b. If the stauts of the VLAN is UP (even if interfaces are disconnected), shutdown the VLAN associated with fe1:

```
RFS7000(config)*#show ip interface brief
 Interface            IP-Address/Mask          Status                Protocol
  fe 157.235.208.122/24(DHCP) up                    up
  vlan1                unassigned(DHCP)         up                     up
  vlan200              unassigned up                    up
 RFS7000(config)*#shutdown
```

   c. Check the status and note if the VLAN has been disassociated. Its status has now changed to DOWN.

```
RFS7000(config)#show ip interface brief
Interface            IP-Address           Status               Protocol
vlan1                157.235.208.69(DHCP)  up                   up
vlan3                unassigned            administratively down down
RFS7000(config)#
```

2. The above instance may occur when a DHCP interface is disconnected. DHCP is not effected because it runs on a virtual interface and not on the physical interface. In this case, it is the physical interface that is disconnected not the virtual interface.
   When the Ethernet interface comes back up, it restarts the DHCP client on any of the virtual interfaces (SVIs) in which the physical interface is a member port. This ensures (if the interface was disconnected and reconnected to a different interface), it gets a new IP address, route, name server, domain name etc. corresponding to the new DHCP server/ scope.

Example

```
RFS7000(config)#  show ip access-list
```

```
Standard IP access list 1
    permit 172.16.10.10/24 rule-precedence 10
RFS7000(config)#

RFS7000(config)#show ip dhcp binding manual
IP              MAC/Client-Id
--              -------------
RFS7000(config)#


RFS7000(config)#show ip dhcp binding
IP              MAC/Client-Id      Type Expiry Time
--              -------------      ---- -----------
RFS7000(config)#

RFS7000#show ip dhcp pool
!
ip dhcp pool pl!
ip dhcp pool pool1
 domain-name test.com
 bootfile 123
 network 10.10.10.0/24
 address range 10.10.10.2 10.10.10.30!
ip dhcp pool poo110
 next-server 1.1.1.1
 netbios-node-type b-node

RFS7000#show ip dhcp-vendor-options
Server Info:
Firmware Image File:
Config File:
Cluster Config File:

RFS7000#show ip domain-name
 IP domain-lookup : Enable
 Domain Name   : symbol.com

RFS7000#show ip http server
HTTP server: Running
Config status: Enabled

RFS7000#show ip http secure-server
HTTP secure server: Running
Config status: Enabled
Trustpoint: default-trustpoint


RFS7000(config)#show ip nat translations outside source
S/D Dir Actual Address              NATed Address          ACL       Overload-If
RFS7000(config)#

RFS7000#show ip routing
IP routing is on

RFS7000#show ip route detail
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
       > - Active route, * - Next-hop in FIB, p - stale info

C    *> 10.1.1.0/24 is directly connected, me1
C    *> 172.16.10.0/24 is directly connected, vlan1
RFS7000#


RFS7000#show ip ssh
SSH server: enabled
Status: running
Keypair name: default_ssh_rsa_key
Port: 22
```

2.1.21 ldap

Show commands common to all modes

Displays *LightWeight Directory Access Protocol* (LDAP) server configuration parameters.

Syntax

```
show ldap [configuration {primary|secondary}]
```

Parameters

ldap [configuration]	Displays LDAP server configuration
primary	Optional. Displays primary LDAP server configuration
secondary	Optional. Displays secondary LDAP server configuration

Example

```
RFS7000(config-radsrv)#show ldap configuration
LDAP Server Config Details
_____________________________

Primary LDAP Server configuration

        IP Address              : 10.10.10.1
        Port                    : 369
        Login                   :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                 : cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                 : ou=symbol,dc=activedirectory,dc=com
        Password                : 0 symbol@123
        Password Attribute      : UserPassword
        Group Name              : cn
        Group Membership Filter: (&(objectClass=group)(member=%{Ldap-UserDn}))
        Group Member Attr       : radiusGroupName
        Net timeout             : 1 second(s)

Secondary LDAP

        IP Address              : 10.10.10.5
        Port                    : 369
        Login                   :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                 : cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                 : ou=symbol,dc=activedirectory,dc=com
        Password                : 0 symbol@123
        Password Attribute      : UserPassword
        Group Name              : cn
        Group Membership Filter: (&(objectClass=group)(member=%{Ldap-UserDn}))
        Group Member Attr       : radiusGroupName
        Net timeout             : 1 second(s)
```

2.1.22 licenses

Show commands common to all modes

Use this command to view installed licenses.

Syntax

```
show licenses
```

Parameters

None

Example

```
RFS7000(config)#show licenses
  feature usage    license string                license value     usage
    AP               2FFD7fE9 CD016155 14A92C70              48       1
```

2.1.23 logging

Show commands common to all modes

Use this command to view logging configuration and buffer.

Syntax

```
show logging
```

Parameters

None

Example

```
RFS7000(config)#show logging

Logging module: enabled
    Aggregation time: disabled
    Console logging: level warnings
    Monitor logging: disabled
    Buffered logging: level warnings
    Syslog logging: disabled

Log Buffer (4165 bytes):
Ü
Sep 02 00:51:58 2011: %KERN-4-WARNING:  DOS: CORRUPT_PACKET: source Interface:vlan1 :
ipproto:6 : Src IP:172.16.10.204 : Dst IP:172.16.10.2 : Src Port 1681: Dst Port 22:
Invalid TCP sequence number.
Ü
Sep 02 00:44:45 2011: %AUTH-3-ERR: sshd[12638]: error: Could not get shadow information
for NOUSER
Ü
Sep 02 00:44:02 2011: %KERN-4-WARNING:  DOS: CORRUPT_PACKET: source Interface:vlan1 :
ipproto:6 : Src IP:172.16.10.204 : Dst IP:172.16.10.2 : Src Port 1627: Dst Port 22:
Invalid TCP sequence number.
Ü
Sep 01 23:50:16 2011: %KERN-4-WARNING:  DOS: CORRUPT_PACKET: source Interface:vlan1 :
ipproto:6 : Src IP:172.16.10.204 : Dst IP:172.16.10.2 : Src Port 1597: Dst Port 22:
Invalid TCP sequence number.

.....
.....

RFS7000(config)#
```

2.1.24 mac

Show commands common to all modes

Use this command to display MAC access lists (ACLs) and access groups.

Syntax

```
show mac [access-group|access-list]
show mac access-group [<IFNAME>|all|ge <1-4>|me1|role <ROLE-NAME>|sa <1-4>|
  vlan <1-4094>]
```

Parameters

access-group [<IFNAME>|all| ge <1-4>|me1| role <NAME>| sa <1-4>|vlan <1-4094>]	Displays MAC ACLs attached to an interface. Select one of the following options: • <IFNAME> - Displays MAC ACLs attached to a specified interface. Specify the interface name. • all - Displays MAC ACLs attached on all interfaces • ge <1-4> - Displays MAC ACLs attached to GigabitEthernet interface. Select the interface index between 1 - 4. • me1- Displays MAC ACLs attached to FastEthernet interface • role <NAME> - Displays MAC ACLs attached to a specified role. Specify the role name. • sa <1-4> - Displays MAC ACLs attached to StaticAggregate interface. Select the interface index between 1 - 4. • vlan <1-4094> - Displays MAC ACLs attached to VLAN interface. Select the interface index between 1 - 4094.
access-list	Displays MAC access lists

Example

```
RFS7000(config)#show mac access-list
RFS7000(config)#
```

2.1.25 mac-address-table

Show commands common to all modes

Use this command to view MAC address table.

Syntax

```
show mac-address-table
```

Parameters

None

Example

```
RFS7000(config)#show mac-address-table
Bridge       VLAN Port         Mac             Fwd
------------ ---- ------------ -------------- ---
1            1    ge1          0002.b328.d155 1
1            1    ge1          0015.7038.064a 1
1            1    ge1          00a0.f868.d55d 1
1            1    ge1          0015.7037.fabf 1
RFS7000(config)#
```

2.1.26 mac-name

Show commands common to all modes

Use this command to view configured MAC names.

Syntax

```
show mac-name
```

Parameters

None

Example

```
RFS7000#show mac-name
Number of MAC names configured = 0
RFS7000#
```

2.1.27 management

Show commands common to all modes

Displays L3 management interface name.

Syntax

```
show management
```

Parameters

None

Example

```
RFS7000(config)#show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
RFS7000(config)#
```

2.1.28 mobility

Show commands common to all modes

Use this cpmmand to view mobility parameters.

Syntax

```
show mobility [event-log|forwarding|global|mobile-unit|peer|statistics]

show mobility event-log [mobile-unit|peer]
show mobility forwarding {<AA-BB-CC-DD-EE-FF>}
show mobility mobile-unit {<AA-BB-CC-DD-EE-FF>|detail}
show mobility peer {<A.B.C.D>|detail}
show mobility statistics {<AA-BB-CC-DD-EE-FF>}
```

Parameters

event-log [mobile-unit|peer]	Displays following mobility event logs: • mobile-unit – *Mobile units* (MU) event logs • peer – Peer event logs
forwarding <AA-BB-CC-DD-EE-FF>	Displays specified MU in the forwarding plane • <AA-BB-CC-DD-EE-FF> – Optional. Specify the mobile unit's MAC address.
global	Displays global mobility parameters
mobile-unit {<AA-BB-CC-DD-EE-FF>| detail}	Displays specified MU in the mobility database • <AA-BB-CC-DD-EE-FF> – Optional. Specify the mobile unit's MAC address. • detail – Optional. Displays detailed information
peer {<A.B.C.D|detail>}	Displays specified mobility peer • <A.B.C.D> – Optional. Specify the peer's IP address. • detail – Optional. Displays detailed information
statistics {<AA-BB-CC-DD-EE-FF>}	Displays specified MU's mobility statistics • <AA-BB-CC-DD-EE-FF> – Optional. Specify the mobile unit's MAC address.

Example

```
RFS7000(config)#show mobility ?
  event-log    Event Log
  forwarding   Mobile-unit information in the forwarding plane
  global       Global Mobility parameters
  mobile-unit  Mobile-units in the Mobility Database
  peer         Mobility peers
  statistics   Mobile-unit Statistics


RFS7000(config)#show mobility global
Mobility Global Parameters
Admin Status                      : DISABLED
Operational-Status                : DISABLED (Admin-status is DISABLED)
Local Address                     : 172.16.10.2 (mgmt-vlan)
Port Number                       : 58788
Max Roam Period                   : 5 sec
Number of Peers                   : 0 (established=0)
Number of MU                      : 0 (Home=0, Foreign=0, Fwding-plane=0, Delete-pend=0)
L3-Mobility enabled WLANs         : NONE
RFS7000(config)#
```

```
RFS7000(config)#show mobility event-log mobile-unit
Time            Event        Evt-Src-IP      MU-Mac             MU-IP
HS-IP           CS-IP
09/14 19:17:52  IP-UPD-MU    n/a             00-0f-3d-e9-a6-54
157.235.208.134 157.235.208.16  157.235.208.16
09/14 19:17:51  ADD-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:51  DEL-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:50  ADD-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16


RFS7000(config)#show mobility forwarding
Mobility Forwarding-plane Information
  State: HS : Home-Switch        CS : Current-Switch
         !HS: Not Home-Switch    !CS: Not Current-Switch
Mac-Address        IP-Address      State   HS-Vlan    Tunnel
RFS7000(config)#


RFS7000(config)#show mobility mobile-unit detail
HOME MU Database: Total=1
MU MAC-Address: 00-0f-3d-e9-a6-54, IP-Address: 157.235.208.134,
SSID=wios_rad_test1
  Home-Switch: 157.235.208.16, Current-Switch: 157.235.208.16, HS-VLAN=1

Foreign MU Database: Total=0

RFS7000(config)#show mobility peer detail
Mobility Peers: Total=1, Established=0
Peer: 1.1.1.1, State: PASSIVE-CONNECTING
  Join-Sent  : 0      Join-Rcvd  : 0      Leave-Sent : 0      Leave-Rcvd : 0
  Rehome-Sent: 0      Rehome-Rcvd: 0      L3roam-Sent: 0      L3roam-Rcvd: 0
  Num-flaps  : 0      Connect-retries: 0    Peer-Uptime: 0 days, 00:00:00

RFS7000(config)#show mobility statistics

MU <00-0f-3d-e9-a6-54> Mob-State HS_AND_CS
-----------------------------------------------
Inter-          |Rx                                        |Tx
face            |unicast    MC         BC         Error     |unicast    MC
BC         Error
wlan_port        0          0          0          0          0          0
0          0
```

2.1.29 ntp

Show commands common to all modes

Use this command to view *Network Time Protocol* (NTP) configuration settings.

Syntax

```
show ntp [associations {detail}|status]
```

Parameters

ntp	Displays NTP settings
association (detail)	Displays NTP associations • detail – Optional. Specify 'detail' to view detailed NTP associations.
status	Displays NTP status

Example

```
RFS7000>show ntp associations
  address         ref clock       st  when  poll  reach  delay  offset    disp
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
RFS7000>(config)#

RFS7000(config)#show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is 2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFS7000(config)#

RFS7000(config)#show ntp associations detail
157.235.208.105 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
our mode client, peer mode unspec, our poll intvl 6, peer poll intvl 10
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
rcv time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
xmt time c8b42a7e.6eb04252 (Sep 14 19:22:38 UTC 2006)
filtdelay =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filtoffset =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filterror =  16000.00  16000.00  16000.00  16000.00  16000.00  16000.00
16000.00  16000.00

RFS7000(config)#show ntp status
Clock is unsynchronized, stratum 16, reference is INIT
actual frequency is 0.0000 Hz, precision is 2**-20
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 1395.000 msec,
```

2.1.30 port

Show commands common to all modes

Use this command to display physical/aggregate port interface.

Syntax

```
show port [fw config]
```

Parameters

fw [config]	Displays configurable firewall parameters

Example

```
RFS7000(config)#show port fw config
IfName | ArpTrust | DhcpTrust | ArpRate | BcastRate | McastRate | UcastRate
=================================================================================
 ge1 |    No |   Yes |     0 |     0 |     0 |     0 |
 ge2 |    No |   Yes |     0 |     0 |     0 |     0 |
 ge3 |    No |   Yes |     0 |     0 |     0 |     0 |
 ge4 |    No |   Yes |     0 |     0 |     0 |     0 |
RFS7000(config)#
```

2.1.31 port-channel

Show commands common to all modes

Syntax

```
show port-channel load-balance
```

Parameters

port-channel load-balance	Displays port channel load balancing configuration

Example

```
RFS7000(config)#show port-channel load-balance
RFS7000(config)#
```

2.1.32 privilege

Show commands common to all modes

Use this command to view current privilege levels.

Syntax

```
show privilege
```

Parameters

None

Example

```
RFS7000>show privilege
Current user privilege: superuser
RFS7000>
```

2.1.33 protocol-list

Show commands common to all modes

Syntax

```
show protocol-list
```

Parameters

None

Example

```
RFS7000>show protocol-list
Protocol Name                    Protocol Number
----------------------------------------
                  ip                    0
                icmp                    1
                igmp                    2
                 ggp                    3
             ipencap                    4
                  st                    5
                 tcp                    6
                 egp                    8
                 igp                    9
                 pup                   12
                 udp                   17
                 hmp                   20
             xns-idp                   22
                 rdp                   27
             iso-tp4                   29
                 xtp                   36
                 ddp                   37
           idpr-cmtp                   38
                ipv6                   41
          ipv6-route                   43
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000>
```

2.1.34 radius

Show commands common to all modes

Use this command to view RADIUS configuration details.

Syntax

```
show radius [configuration|eap|group|nas|proxy|rad-user|trust-point]

show radius eap [configuration]
show radius group {<WORD>}
show radius nas {<A.B.C.D/M>}
show radius proxy {<WORD>}
show radius rad-user {<WORD>}
```

Parameters

radius	Displays RADIUS configuration commands
configuration	Displays RADIUS server configuration parameters
eap [configuration]	Displays EAP parameters and configuration
group {<WORD>}	Displays existing RADIUS group configuration • <WORD> – Optional. Specify the RADIUS group (should exist in the local RADIUS database).
nas {<A.B.C.D/M>}	Displays client information • <A.B.C.D/M> – Optional. Enter the client's IP address and mask.
proxy {<WORD>}	Displays proxy information • <WORD> – Optional. Specify the proxy realm name.
rad-user {<WORD>}	Displays RADIUS user information • <WORD> – Optional. Specify RADIUS user name (should exist in the local RADIUS database).
trust-point	Displays RADIUS trustpoint configuration

Example

```
RFS7000(config)#show radius proxy
Proxy Details

_______________
Proxy retry delay : 5  seconds
Proxy retry count : 3

%No realm configured

RFS7000(config)#
```

2.1.35 redundancy

Show commands common to all modes

This command displays the switch's IP address, number of active neighbors, group license, installed license, cluster AP adoption count, switch adoption count, hold time, discovery time, heartbeat interval, cluster id, switch mode etc.

In a cluster, this command displays the redundancy runtime and configured information of the self-switch. Use `config` parameter to view only configuration information and/or `runtime` parameter to view runtime information.

Syntax

```
show redundancy [dynamic-ap-load-balance|group|history|members]
show redundancy dynamic-ap-load-balance [config]
show redundancy group {config|runtime}
show redundancy members {<A.B.C.D>|brief}
```

Parameters

dynamic-ap-load-balance [config]	Displays redundancy dynamic AP load balance parameters • config – Displays dynamic AP load balancing configuration
group {config|runtime}	Displays redundancy group parameters • config – Optional. Displays configured redundancy group information • runtime – Optional. Displays runtime redundancy group information
history	Displays state transition history of the switch
members {<A.B.C.D>|brief}	Displays redundancy group members in detail • <A.B.C.D> – Optional. Specify the IP address of the member switch. • brief – Optional. Displays members in brief

Example

```
RFS7000(config)#show redundancy members brief

Member ID (Self)              : 0.0.0.0
Member State                  : Not Applicable
RFS7000(config)#

RFS7000(config)#show redundancy dynamic-ap-load-balance config
Dynamic AP Load Balance Configuration:
  Load balance          : Disabled
  Load balance trigger  : Schedule

Dynamic AP Load Balance Schedule:
  Schedule first-time   : Sun Jun  1 00:00:00 2008
  Schedule interval     : 1 day(s)

Per AP MU Threshold     : 32
RFS7000(config)#
```

2.1.36 role

Show commands common to all modes

Use this command to view configured role parameters.

Syntax

```
show role {<ROLE-NAME>|mobile-units}
```

Parameters

role	Displays configured role parameters
<ROLE-NAME>	Optional. Displays configured role parameters for an existing role. Specify the existing role name.
mobile-units	Optional. Displays mobile units assigned to these roles

Example

```
RFS7000#show role mobile-units
MU's present in role = default-role
RFS7000#

RFS7000(config)#show role

role default-role 10001
 authentication-type any
 encryption-type any
 ap-location any
 essid any
 mu-mac any
 group any
RFS7000(config)#
```

2.1.37 rtls

Show commands common to all modes

Syntax2

```
show rtls [aeroscout|ekahau|filter|site|sole|tags|zone]

show rtls [aeroscout|ekahau|filter {<1-100>}|site|sole {peers|probes}|
  tags {aeroscout|all|ekahau|g2|mobile-unit|rfid|zone}|zone {<1-48>|(detail}]
```

Parameters

aeroscout	Displays AeroScout configurations
ekahau	Displays ekahau configurations
filters <1-100>	Displays RFID tag filters • <1-100> – Optional. Select the tag filter index between 1 - 100.
site	Displays site configurations

sole {peers|probes}	Displays SOLE configurations
	• peers – Optional. Displays SOLE peer information
	• probes {<AA-BB-CC-DD-EE-FF>|aeroscout|ekahau|mobile-unit} – Optional. Displays probe information based on the option selected. The options are:
	  • <AA-BB-CC-DD-EE-FF> – Specify the MAC address to view probes.
	  • aeroscout – Displays AeroScout probes
	  • ekahau – Displays ekahau probes
	  • mobile-units – Displays mobile unit probes

tags {aeroscout|all| ekahau|g2| mobile-unit|rfid|zone}	Displays tags/assets (passive, active, wi-fi) information • aeroscout {all} – Optional. Displays AeroScout tags • all – Displays all tags • ekahau {all} – Optional. Displays ekahau tags • g2 {all} – Optional. Displays located G2 tags • mobile-unit {all}– Optional. Displays located mobile units (802.11 clients) • rfid {all} – Optional. Displays located RFID gen2 tags. • zone <1-48> {all} – Optional. Displays zone configuration for a specified zone index. Specify the zone index between 1 - 48. • {all} – Optional. Displays all tags based on the option selected
zone {<1-48>|detail}	Displays zone statistics • <1-48> – Optional. Specify the zone index between 1 - 48. • detail – Optional. Displays zone details

Example

```
RFS7000#show rtls aeroscout
Type                : aeroscout
On-board            : enabled
Interval            : 5(s)
External            : disabled
Engine IP           : ------
Port                : 0
```

```
Recv msg count      : 0
Sent msg count      : 0
Tag report count    : 0
Last msg recv time  : -
Last msg sent time  : -
RFS7000#
```

2.1.38 service-list

Show commands common to all modes

Use this command to display list of services.

Syntax

```
show service-list
```

Parameters

None

Example

```
RFS7000#show service-list
Service Name                      Port Number
-----------------------------------------
              tcpmux                    1/tcp
                rtmp                    1/ddp
                 nbp                    2/ddp
                echo                    4/ddp
                 zip                    6/ddp
                echo                    7/tcp
                echo                    7/udp
             discard                    9/tcp
             discard                    9/udp
              systat                   11/tcp
             daytime                   13/tcp
             daytime                   13/udp
             netstat                   15/tcp
                qotd                   17/tcp
                 msp                   18/tcp
                 msp                   18/udp
             chargen                   19/tcp
             chargen                   19/udp
           ftp-data                    20/tcp
                ftp                    21/tcp
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000#
```

2.1.39 smtp-notification

Show commands common to all modes

Use this command to display SNMP engine parameters.

Syntax

```
show smtp-notification (traps)
```

Parameters

traps	Displays Trap enable flags

Example

```
RFS7000#show smtp-notification traps

-------------------------------------------------------------------------
Global enable flag for Trap SMTP-Notification           Disabled
-------------------------------------------------------------------------


Enable flag status for Individual Trap SMTP-Notification
-------------------------------------------------------------------------
Module Type               Trap Type                  Enabled?[Y/N]
-------------------------------------------------------------------------
snmp                     coldstart                                N
snmp                     linkdown                                 N
snmp                     linkup                                   N
snmp                     authenticationFail                       N
nsm                      dhcpIPChanged                            N
diagnostics              tempHigh                                 N
diagnostics              tempOver                                 N
diagnostics              fanSpeedLow                              N
diagnostics              cpuLoad1Min                              N
diagnostics              cpuLoad5Min                              N
diagnostics              cpuLoad15Min                             N
diagnostics              usedKernelBuffer                         N
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000#RFS7000#
```

2.1.40 snmp

Show commands common to all modes

Use this command to view *Simple Network Management Protocol* (SNMP) engine configuration.

Syntax

```
show snmp user [snmpmanager|snmpoperator|snmptrap]
```

Parameters

user	Displays SNMP user information. The user options are: • SNMP manager • SNMP operator • SNMP trap user
snmpmanager	Displays snmp manager information
snmpoperator	Displays snmp operator information
snmptrap	Displays SNMPsnmp trap user information

Example

```
RFS7000#show snmp user snmpmanager
userName      access   engineId                    Authentication  Encryption
snmpmanager   rw       80000184806b8b45674e5872c3  SHA             AES
RFS7000#
```

2.1.41 snmp-server

Show commands common to all modes

Use this command to display SNMP engine parameters.

Syntax

```
show snmp-server {traps {wireless-statistics [mesh|mobile-unit|radio|
  wireless-switch|wlan]}}
```

Parameters

snmp-server	Displays SNMP server status and version. To view SNMP server trap flags, select traps parameter.
traps	Optional. Displays trap enable flags
wireless-statistics	Optional. Displays wireless stats rate traps, based on the option selected
mesh	Displays mesh rate traps
mobile-unit'	Displays mobile unit rate traps
radio	Displays radio rate traps
wireless-switch	Displays wireless switch rate traps
wlan	Displays WLAN rate traps

Example

```
RFS7000#show snmp-server traps wireless-statistics radio
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     avg-bit-speed-less-than                  disabled
     avg-signal-less-than                     disabled
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
     num-mobile-units-greater-than            disabled
     avg-noise-level-threshold                disabled
RFS7000#
```

2.1.42 spanning-tree

Show commands common to all modes

Use this command to view spanning tree configuration.

Syntax

```
show spanning-tree mst {configuration|detail|instance}

show spanning-tree mst {detail {interface [<IFNAME>|ge <1-4>|me1|sa <1-4>|
  vlan <1-4094>]}}

show spanning-tree mst {instance [<1-15>] {interface [<IFNAME>|ge <1-4>|me1|
  sa <1-4>|vlan <1-4094>]}}
```

Parameters

mst (configuration)	
configuration	Optional. Displays spanning-tree MST configuration information
mst (detail)	
detail {interface} [<IFNAME>| ge <1-4>|me1| sa <1-4> | vlan <1-4094>]	Optional. Displays detailed interface information based on the option selected. Select the interface type. • <IFNAME> - Displays spanning-tree MST information for a specified interface. Specify the interface name. • ge <1-4> - Displays spanning-tree MST information for GigabitEthernet interface. Select the interface index between 1 - 4. • me1 - Displays spanning-tree MST information for FastEthernet interface. • sa <1-4> - Displays spanning-tree MST information for StaticAggregate interface. Select the interface index between 1 - 4. • vlan <1-4094> - Displays spanning-tree MST information for VLAN interface. Select the VLAN interface ID between 1 - 4094.
mst (instance)	
instance <1-15> {interface} [<IFNAME>| ge <1-4>|me1| sa <1-4> | vlan <1-4094>]	Optional. Displays interface instance information. Select the interface instance index between 1 - 15. • <IFNAME> - Displays spanning-tree MST information for a specified interface instance. Specify the interface name. • ge <1-4> - Displays spanning-tree MST information for GigabitEthernet interface instance. Select the interface index between 1 - 4. • me1 - Displays spanning-tree MST information for FastEthernet interface instance • sa <1-4> - Displays spanning-tree MST information for StaticAggregate interface instance. Select the interface index between 1 - 4. • vlan <1-4094> - Displays spanning-tree MST information for VLAN interface instance. Select the VLAN interface ID between 1 - 4094.

Example

```
RFS7000>show spanning-tree mst configuration
%
%  MSTP Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0xAC36177F50283CD4B83821D8AB26DE62
%-------------------------------------------------------
RFS7000>

RFS7000>show spanning-tree mst detail interface ge 3
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000001570380843
% 1: CIST Reg Root Id 8000001570380843
% 1: CST Bridge Id 8000001570380843
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability configured - Current cisco interoperability off
%   ge3: Port 2003 - Id 87d3 - Role Disabled - State Discarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 0
%   ge3: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge3: Designated Port Id 0 - CST Priority 128  -
%   ge3: CIST Root 0000000000000000
%   ge3: Regional Root 0000000000000000
%   ge3: Designated Bridge 0000000000000000
%   ge3: Message Age 0 - Max Age 0
%   ge3: CIST Hello Time 0 - Forward Delay 0
%   ge3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge3: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge3: No portfast configured - Current  portfast off
%   ge3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current  shared

RFS7000>
```

2.1.43 static-channel-group

Show commands common to all modes

Use this command to view static channel group membership.

Syntax

```
show static-channel-group
```

Parameters

None

Example

```
RFS7000>show static-channel-group
RFS7000>
```

2.1.44 terminal

Show commands common to all modes

Use this command to view terminal configuration parameters.

Syntax

```
show terminal
```

Parameters

None

Example

```
RFS7000>show terminal
Terminal Type: xterm
Length: 24     Width: 80
RFS7000>
```

2.1.45 timezone

Show commands common to all modes

Use this command to display the timezone.

Syntax

```
show timezone
```

Parameters

None

Example

```
RFS7000>show timezone
Timezone is Etc/UTC
RFS7000>
```

2.1.46 traffic shape

Show commands common to all modes

Use this command to display traffic shaping.

Syntax

```
show traffic-shape [config|priority-map|statistics]
show traffic-shape [config {class <1-4>}|priority-map|statistics {class <1-4>}]
```

Parameters

config {class <1-4>}	Displays traffic shaping configuration for a specified traffic shaping class. • class <1-4> – Optional. Specifies the traffic shaping class number between 1 - 4.
priority-map	Displays 1p to transmit priority map.
statistics {class <1-4>}	Displays traffic shaping statistics for a specified traffic shaping class • class <1-4> – Optional. Specifies the traffic shaping class number between 1 - 4.

Example

```
RFS7000#show traffic-shape priority-map
 802.1p | Shaping priority
      0  |  2
      1  |  0
      2  |  1
      3  |  3
      4  |  4
      5  |  5
      6  |  6
      7  |  7
RFS7000#
```

2.1.47 users

Show commands common to all modes

Use this command to view information about currently logged in users.

Syntax

```
show users
```

Parameters

None

Example

```
RFS7000(config)#show users
   Line      PID   User         Uptime       Location
 130 vty 0  14386   admin         00:45m        0
RFS7000(config)#
```

2.1.48 version

Show commands common to all modes

Use this command to display software and hardware version.

Syntax

```
show version {verbose}
```

Parameters

verbose	Optional. Displays software and hardware details

Example

```
RFS7000(config)#show version
RFS7000 version 4.1.2.0-007GD
Copyright (c) 2006-2011 Motorola Solutions, Inc.
Booted from primary.

Switch uptime is 6 days, 15 hours 39 minutes
CPU is RMI XLR V0.4
255484 kB of on-board RAM
RFS7000(config)#


RFS7000(config)#show version verbose
RFS7000 version 4.1.2.0-007GD
Copyright (c) 2006-2011 Motorola Solutions, Inc.
Booted from primary.

Switch uptime is 6 days, 15 hours 40 minutes
CPU is RMI XLR V0.4
PCI bus 0 device 3 function 2
    USB Controller
    unknown mfg
    unknown
PCI bus 0 device 3 function 1
    USB Controller
    unknown mfg
    unknown
PCI bus 0 device 3 function 0
    USB Controller
    unknown mfg
    unknown
PCI bus 0 device 1 function 0
    Ethernet controller
    unknown mfg
    unknown
255484 kB of on-board RAM
RFS7000(config)#
```

2.1.49 virtual ip

Show commands common to all modes

Use this command to display IP redundancy features.

Syntax

```
show virtual-ip [config|status]
```

Parameters

config	Displays configuration details
status	Displays current status

Example

```
RFS7000#show virtual-ip config
Virtual-IP Status            : Disabled
Cluster Redundancy Status    : Disabled
Priority Selection Mode      : Automatic
Learning Timeout(sec)        : 2
Advertisement Timeout(sec)   : 1
Gratuitous ARP Timeout(sec)  : 180
Virtual-IP Server Port       : 51525
Switch IP                    : 0.0.0.0
Reserved VMAC Address Range  : 00-15-70-88-8A-90 to 00-15-70-88-8B-8F
Configured Virtual MAC       : Not Configured
DHCP Server status           : Not Running on this Switch
+-------------------------------------------------+
| Vlan |  Priority  |    SwitchID   |  Virtual IP   |
---------------------------------------------------+
|                                                 |
+-------------------------------------------------
RFS7000#
```

2.1.50 wireless

Show commands common to all modes

Syntax

```
show wireless [aap-version|ap|ap-containment|ap-detection-config|
  ap-images|ap-radio-config|ap-unadopted|authorized-aps|
  channel-power|client|config|country-code-list|default-ap|fw|
  fwupdate-filelocation|fwupdate-filename|fwupdate-mode|fwupdate-serveraddress|
  fwupdate-username|hotspot|hotspot-config|ignored-aps|know|
  mac-auth-local|mesh|mobile-unit|multicast-packet-limit|
  non-preferred-ap-attempts-threshold|qos-mapping|radio|radio-group|
  regulatory|self-heal-config|sensor|smart-rf|unauthorized-aps|
  wips|wireless-switch-statistics|wlan]

show wireless aap-version

show wireless ap {<LIST>|config (<1-1024>|<LIST>)}

show wireless ap-containment [config|table]

show wireless ap-detection-config

Show wireless ap-images

show wireless ap-radio-config <AA-BB-CC-DD-EE-FF>

show wireless ap-unadopted

show wireless authorized-aps

show wireless channel-power [11a|11b|11bg] (indoor|outdoor)

show wireless client [exclude-list|include-list]

show wireless config

show wireless country-code-list

show wireless default-ap

show wireless fw [config]

show wireless fwupdate-filelocation

show wireless fwupdate-filename

show wireless fwupdate-mode

show wireless fwupdate-serveraddress

show wireless fwupdate-username

show wireless hotspot [query]

show wireless hotspot-config <1-256>

show wireless ignored-aps

show wireless known {ap statistics {<1-1024>}}
show wireless mac-auth-local {<1-1000>}

show wireless mesh [statistics] {<1-32>} {detail}

show wireless mobile-unit {<1-8192>|<AA-BB-CC-DD-EE-FF>|
  association-history <AA-BB-CC-DD-EE-FF>|association-stats|
  probe-history [<1-200>|config-list]|radio <1-4096>|
  roaming [database]|statistics [<1-8192>|<AA-BB-CC-DD-EE-FF> (detail)|summary|
  voice (<1-8192>|<AA-BB-CC-DD-EE-FF>)]|wlan <WLAN-RANGE>}

show wireless multicast-packet-limit
```

```
show wireless non-preferred-ap-attempts-threshold

show wireless qos-mapping {wired-to-wireless|wireless-to-wired}

show wireless radio {<1-4096>|admission-control [voice] {<1-4096>}|all|beacon-table|
  config (<1-4096>|default-11a|default-11an|default-bg|default-bgn)|
  monitor-table|statistics (<1-4096>|long-interval|short-interval|voice)|
  unadopted|uptime|voice <1-4096>}

show wireless radio-graoup <1-256>

show wireless regulatory (country codes)

show wireless self-heal-config {<1-4096>|all}

show wireless sensor {<1-48>|default-config}

show wireless smart-rf [calibration-status|configuration|history|radio]
show wireless smart-rf radio [config|local-status|map|master-status|neighbors|spectrum]
show wireless smart-rf radio [config|local-status] {<1-4096>|<AA-BB-CC-DD-EE-FF>|
  all-11a|all-bg}
show wireless smart-rf radio [map|master-status}neighbors|spectrum]
  {<AA-BB-CC-DD-EE-FF>|all-11a|all-bg}

show wireless unauthorized-aps

show wireless wips {configured-ap-def-essids|configured-bad-essids|
  fake-ap-flood [threshold]|filter-list|suspicious-ap [signal-strength-threshold]}

show wireless wireless-switch-statistics {detail}

show wireless wlan [config {<1-256>|all|enabled)|statistics {<1-256> detail}]
```

Parameters

wireless (aap-version)	
aap-version	Displays the minimum adaptive firmware version
wireless (ap)	

ap {<LIST>|config}	Displays status of adopted access port
	• <LIST> – Optional. Displays detailed information for a single port or a list of ports (for example, 1-4, 10).
	• config {<1-1024>|<LIST>} – Optional. Displays access port status
	  • <1-1024> – Optional. Specify a single access port index between 1 -1024
	  • <LIST> – Optional. List access port MAC addresses (for example, 1-4, 10)
	Note: Use the `show wireless ap` command to view access port indices.

wireless (ap-containment)	
ap-containment (config|table)	Displays rogue AP containment information • config – Displays rogue AP containment parameters • table – Displays rogue AP containment table

wireless (ap-detection-config)	
ap-detection-config	Displays detected AP configuration parameters
wireless (ap-images)	
ap-images	Lists the access port images on the wireless switch
wireless (ap-radio-config)	
ap-radio-config	Displays AP radio configurations
wireless (ap-unadopted)	
ap-unadopted	Lists unadopted access ports
wireless (authorized-aps)	
authorized-aps	Displays authorized APs seen by access port scans
wireless (channel-power)	

channel-power [11a|11b|11bg]	Displays a list of available channel and power levels for a radio
	• 11a – Radio is 802.11a
	• 11b – Radio is 802.11b.
	• 11bg – Radio is 802.11bg
	  • indoor – Radio is placed indoors
	  • outdoor – Radio is placed outdoors

wireless (client)	
client	Displays wireless client configuration • exclude-list – Displays exclude list configuration • include-list – Displays include list configuration
wireless (config)	
config	Displays wireless configuration parameters
wireless (country-code-list)	
country-code-list	Displays a list of supported country names and 2 letter ISO 3166 codes
wireless (default-ap)	
default-ap	Displays default access port information
wireless (fw)	
fw (config)	Displays configurable Firewall parameters
wireless (fwupdate-filelocation)	

fwupdate-filelocation	Displays file location
wireless (fwupdate-name)	
fwupdate-filename	Displays file name
wireless (fwupdate-mode)	
fwupdate-mode	Displays firmware upgrade mode
wireless (fwupdate-serveraddress)	
fwupdate-serveraddress	Displays SFTP server IP address
wireless (fwupdate-username)	
fwupdate-username	Displays login user name
wireless (hotspot)	
hotspot	Displays hotspot configuration
wireless (hotspot-config)	
hotspot-config {<1-256>}	Displays WLAN hotspot configuration • <1-256> – Optional. Specify the WLAN index between 1 - 256.
wireless (ignored-aps)	
ignored-aps	Displays ignored APs seen by access port scans
wireless (know)	

know {ap}	Displays known AP related parameters
	• ap [statistics] – Optional. A known AP index <1 - 1024>
	  • statistics {<1-1024>} – Known adaptive AP statistics
	  • <1-1024> – Optional. Displays one or more adaptive AP known AP statistics

wireless (mac-auth-local)	
mac-auth-local {<1-1000>}	Lists out the mac-auth-local entries • <1-1000> – Optional. Displays mac-auth-local entry

wireless (mesh)

mesh [statistics] {<1-32>}	Displays mesh related parameters • statistics {<1-32>} – Displays mesh statistics for a specified mesh • <1-32> {detail}– Optional. Select the mesh index between 1 - 32. • detail – Optional. Provides detailed statistics for the mesh specified by the <1-32> parameter.
wireless (mobile-unit)	
mobile-unit {<1-8192>| <AA-BB-CC-DD-EE-FF>| association-history| association-stats| probe-history| radio| roaming|statistics| voice|wlan}	Displays details of associated mobile unit based on the option selected • <1-8192> – Optional. Specify the mobile unit index. • <AA-BB-CC-DD-EE-FF> – Optional. Specify the MAC address of mobile unit. • association-history {<AA-BB-CC-DD-EE-FF>} – Optional. Displays mobile unit history. Enter the mobile unit MAC address in the AA-BB-CC-DD-EE-FF format. • association-stats – Optional. Displays statistics of associations and reassociations • probe-history [<1-20>|config-list] – Optional. Displays MU probe-history based on the option selected • <1-200> – Select the index to display probe logging. • config-list – Lists probe history MAC addresses • radio [<1-4096>] – Optional. Displays mobile units associated with this radio. Select the radio index between 1 - 4096. • roaming [database] – Optional. Displays MU inter-switch roaming database • statistics {<1-8192>|<AA-BB-CC-DD-EE-FF>|summary|voice} – Optional. Displays MU RF statistics of all currently associated mobile units • <1-8192> – Optional. Specify MU index between 1 - 8192. • <AA-BB-CC-DD-EE-FF> (detail) – Optional. Displays detailed MU statistics. Specify MAC address of mobile unit. • summary – Optional. Displays RF statistics summary of all currently associated MUs • voice (<1-8192>|<AA-BB-CC-DD-EE-FF>) – Optional. Displays MU voice statistics. Select the MU by specifying its index or MAC address. • voice – Optional. Displays voice call details • wlan <WLAN_RANGE> – Optional. Displays MUs associated to this WLAN. Select the WLAN index between 1 - 256.
wireless (multicast-packet-limit)	
multicast-packet-limit	Displays multicast packet limit
wireless (non-preferred-ap-attempts-threshold)	

non-preferred-ap-attempts-threshold	Displays non-preferred AP threshold
wireless (qos-mapping)	
qos-mapping {wired-to-wireless| wired-to-wired}	Displays *Quality of Service* (QoS) mappings used for mapping WMM access categories and 802.1p / DSCP tags • wired-to-wireless – Optional. Displays mappings used when traffic is switched from wired to the wireless side • wireless-to-wired – Optional. Displays mappings used when traffic is switched from wireless to the wired side
wireless (radio)	

radio {<1-4096>| admission-control|all| beacon-table|config| monitor-table| statistics|unadopted| uptime|voice}	Displays radio related commands. Select one of the following options:
	• <1-4096> – Optional. A single radio index
	• admission-control – Optional. Displays admission control statistics
	• all – Optional. Displays status of adopted and unadopted radios
	• beacon-table – Optional. Displays the radio-to-radio beacon table
	• config {<1-4096>|default-11a|default-11an|default-11bg| default-11bgn} – Optional. Displays radio configuration based on the option selected. The options are:
	  • <1-4096> – Optional. Displays radio configuration for a specified radio. Select the radio index between 1 - 4096.
	  • default-11a – Optional. Displays default 11a configuration template
	  • default-11an – Optional. Displays default 11an configuration template
	  • default-11bg – Optional. Displays default 11bg configuration template
	  • default-11bgn – Optional. Displays default 11bgn configuration template
	• monitor-table – Optional. Displays the radio-to-radio monitoring table.statistics {<1-4096>|long-interval|shot-interval|voice} – Optional. Displays radio statistics based on the option selected
	  • <1-4096> – Optional. Displays statistics for a specified radio. Select the radio index between 1 - 4096.
	  • long-interval – Optional. Displays summary stats of the last 60 minutes from all adopted radios
	  • short-interval – Optional. Displays summary stats of the last 30 seconds from all adopted radios
	  • voice – Optional. Displays voice related statistics
	• unadopted – Optional. Lists unadopted radios
	• uptime – Optional. Displays uptime of all adopted radios
	• voice {<1-4096>} – Optional. Displays voice call details
	  • <1-4096> – Optional. Displays voice call details for a specified radio. Select the radio index between 1 - 4096.

wireless (regulatory)	
regulatory <WORD>	Displays regulatory (allowed channel/power) information for a particular country • <WORD> – Specify the two letter ISO-3166 country code. (Use the 'show wireless country-code-list' command to list supported country codes.)
wireless (self-heal-config)	
self-heal-config {<1-4096>|all}	Displays self healing configuration parameters • <1-4096> – Optional. Displays self healing configuration for a specified radio. Select the radio index between 1 - 4096. • all – Optional. Displays self healing configuration for all configured radios
wireless (sensor)	
sensor {<1-48>|default-config}	Displays *Wireless Intrusion Protection System* (WIPS) parameters. Use "sensor vlan x" to specify the VLAN(s) to which the sensors are connected. • <1-48> – Optional. Displays WIPS configuration for a specified sensor. Specify the sensor index between 1 - 48. • default-config – Optional. Displays default configuration parameters for sensors
wireless (smart-rf)	

smart-rf [calibration-status| configuration| history|radio]	Displays Smart-RF management commands
	• calibration-status – Displays Smart-RF calibration status
	• configuration – Displays Smart-RF configuration
	• history – Displays Smart-RF assignment history since latest calibration
	• radio – Displays Smart-RF radio related commands. Select one of the following options:
	  • config – Displays local radio config related to Smart-RF
	  • local-status – Displays local radio status related to Smart-RF
	  • map – Displays 11a radios currently in configuration
	  • master-status – Displays radio status from master radio list, all radios ID not specified
	  • neighbors – Displays a radio's neighbor information
	  • spectrum – Displays all 11a radios currently in configuration
	The following keywords are common to the above 'radio' parameters:
	• <1-4096> – A single radio index
	• <AA-BB-CC-DD-EE-FF> – The radio MAC address in the AA-BB-CC-DD-EE-FF format (will consider all radios if no MAC address is specified)
	• all-11a – All 11a radios currently in configuration
	• all-11bg – All 11bg radios currently in configuration

wireless (unauthorized-aps)	
unauthorized-aps	Displays unauthorized APs seen by access port or mobile unit scans
wireless (wips)	
wips {configured-ap-def-essids| configured-bad-essids| fake-ap-flood| filter-list|suspicious-ap}	Displays WIPS parameters based on the option selected • configured-ap-def-essids – Optional. Lists configured default ESSIDs • configured-bad-essids – Optional. Lists configured bad ESSIDs • fake-ap-flood [threshold] – Optional. Displays Fake-AP Flood threshold. • filter-list – Optional. Lists currently filtered mobile units • suspicious-ap [signal-strength-threshold] – Optional. Displays suspicious AP signal strength threshold
wireless (wireless-switch-statistics)	
wireless-switch-statistics {detail}	Displays switch statistics • detail – Optional. Displays detailed switch statistics
wireless (wlan)	

wlan [config|statistics]	Displays Wireless LAN related parameters
	• config {<1-256>|all|enabled} – Optional. Displays WLAN configuration based on the option selected
	  • <1-256> – Optional. Specify the WLAN index between 1 - 256.
	  • all – Displays all WLANs in configuration.enabled – Optional. Displays currently enabled WLANs only
	• statistics {<1-256>} – Optional. Displays statistics for a specified WLAN. Specify the WLAN index
	  • <1-256> {detail} – Optional. Displays detailed statistics for a specified WLAN

Example

```
RFS7000>show wireless ap
Number of access-ports adopted   : 0
Number of AAPs adopted           : 0
Available AP licenses            : 0
Available AAP licenses           : 0
Redundancy enabled               : N
Redundancy mode                  : active
RFS7000>
```

```
RFS7000>show wireless ap-detection-config
Rogue    AP timeout      : 300 seconds
Authorized AP timeout    : 300 seconds
Ignored AP timeout       : 300 seconds
mu-assisted scan         : disabled
mu-assisted scan refresh : 1800 seconds
configured authorized-aps  :
Index | Bss Mac           | Ssid
-----------------------------------------------------
configured ignored-aps  :
Index | Bss Mac           | Ssid
-----------------------------------------------------
AP7131  minimum adoption version: 4.0.0.0-035GR
RFS7000>

RFS7000>show wireless ap-images
  Idx   ap-type      Image-Name         Size (bytes)  Version
   1    ap300     AP300-WISP              293528      00.02-31
   2    ap300     AP300-WISPe             319812      01.00-2290rRFS7000>
RFS7000>show wireless ap-unadopted
RFS7000>


RFS7000>show wireless authorized-aps
AP detection is disabled
RFS7000>


RFS7000>show wireless channel-power 11a indoor
% Error: No valid channels or power levels
RFS7000>

RFS7000(config)#show wireless config
country-code             : us
adoption-pref-id         : 1
proxy-arp                : enabled
adopt-unconf-radio       : enabled
dot11-shared-key-auth    : disabled
ap-detection             : disabled
manual-wlan-mapping      : disabled
dhcp sniff state         : disabled
dhcp fix broadcast-rsp   : disabled
broadcast-tx-speed       : optimize-for-range
wlan bw allocation       : disabled
Adaptive ap parameters:
 local-bridging          : disabled
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
dn-link rate limit /usr : unlimited
up-link rate limit /usr : unlimited
RFS7000(config)#
```

```
RFS7000>show wireles hotspot-config

WLAN: 1, status: disabled, description: WLAN1, ssid: 101
 authentication-type: dot11i pre-shared key, encryption-type: none
 wlan not setup for hotspot

WLAN: 2, status: disabled, description: WLAN2, ssid: 102
 authentication-type: dot11i pre-shared key, encryption-type: none
 wlan not setup for hotspot

WLAN: 3, status: disabled, description: WLAN3, ssid: 103
 authentication-type: dot11i pre-shared key, encryption-type: none
 wlan not setup for hotspot

WLAN: 4, status: disabled, description: WLAN4, ssid: 104
 authentication-type: dot11i pre-shared key, encryption-type: none
 wlan not setup for hotspot

WLAN: 5, status: disabled, description: WLAN5, ssid: 105
 authentication-type: dot11i pre-shared key, encryption-type: none
 wlan not setup for hotspot

WLAN: 6, status: disabled, description: WLAN6, ssid: 106

.....................................................

RFS7000#show wireless aap-version
AAP7131 Version: 4.0.0.0-035GR
RFS7000#
```

2.1.51 wlan-acl

Show commands common to all modes

Use this command to view WLAN based ACLs.

Syntax

```
show wlan-acl [<1-256>|all]
```

Parameters

<1-256>	Displays ACLs attached to the specified WLAN ID. Specify the WLAN ID between 1 - 256.
all	Displays all ACLs attached to the WLAN port

Example

```
RFS7000>show wlan-acl 200
WLAN port: 200
  Inbound IP Access List   :
  Inbound MAC Access List  :
  Outbound IP Access List  :
  Outbound MAC Access List :
RFS7000>

RFS7000>show wlan-acl all
RFS7000>
```

2.1.52 access-list

Show commands in PrivExec and Global Config modes

This command lists all the access lists (numbered and named) configured on the switch. The numbered access list displays all numbered ACLs. The named access-list displays the details of the name ACL.

Syntax

Parameters`show access-list {<1-99>|<100-199>|<1300-1999>|<2000-2699>|<WORD>}`

<1-99>	Optional. Displays IP standard access list
<100-199>	Optional. Displays IP extended access list
<1300-1999>	Optional. Displays IP standard access list (expanded range)
<2000-2699>	Optional. Displays IP extended access list (expanded range)
<WORD>	Optional. Displays a specified ACL. Specify the ACL name.

Example

```
RFS7000(config)#show access-list
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFS7000(config)#


RFS7000(config)#show access-list 110
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFS7000(config)#
```

2.1.53 aclstats

Show commands in PrivExec and Global Config modes

This command displays the statistics of all the access lists configured on the switch.

Syntax

```
show aclstats [access-list|vlan]
show aclstats access-list {<1-99>|<100-199>|<1300-1999>|<2000-2699>|<WORD>}
show aclstats vlan <1-4094>
```

Parameters

access-list	Displays configured access-list statistics • <1-99> – Optional. Displays IP standard access list statistics • <100-199> – Optional. Displays IP extended access list statistics • <1300-1999> – Optional. Displays IP standard access list (expanded range) statistics • <2000-2699> – Optional. Displays IP extended access list (expanded range) statistics • <WORD> – Optional. Displays a specified access list statistics. Specify the ACL name
vlan	Displays access list statistics for a specified VLAN interface • <1-4094> – Specify the VLAN interface between 1 - 4094.

Example

```
RFS7000(config)#show aclstats vlan 4000
RFS7000(config)#show aclstats vlan ?
  <1-4094>  Vlan Id

RFS7000(config)#show aclstats vlan 4000
RFS7000(config)#
```

2.1.54 boot

Show commands in PrivExec and Global Config modes

Use this command to view boot configuration details.

Syntax

```
show boot
```

Parameters

None

Example

```
RFS7000#show boot

Image           Build Date              Install Date          Version
-----       --------------------    --------------------      --------------
Primary     Sep 24 06:24:14 2011     unknown                  4.1.2.0-007GD
Secondary   Sep 24 06:24:14 2011     unknown                  4.1.2.0-007GD

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
RFS7000#
```

2.1.55 clock

Show commands in PrivExec and Global Config modes

Use this command to display the system clock.

Syntax

```
show clock
```

Parameters

None

Example

```
RFS7000#show clock
Sep 03 20:26:35 UTC 2011
RFS7000#
```

2.1.56 debugging

Show commands in PrivExec and Global Config modes

Use this command to view *Multiple Spanning Tree Protocol* (MSTP) information.

Syntax

```
show debugging [stp]
```

Parameters

mstp	Displays MSTP debugging information

Example

```
RFS7000#show debugging mstp
MSTP debugging status:
RFS7000#
```

2.1.57 dhcp

Show commands in PrivExec and Global Config modes

Use this command to display DHCP server configurations.

Syntax

```
show dhcp [config|status]
```

Parameters

config	Displays DHCP server configuration
status	Displays whether the DHCP server is running or not

Example

```
RFS7000#show dhcp config

service dhcp
!
ip dhcp pool vlan63
 default-router 192.168.157.2
 network 192.168.63.0/24
 address range 192.168.63.20 192.168.63.30

RFS7000#
RFS7000#show dhcp status

DHCP Server is Not Running

RFS7000#
```

2.1.58 file

Show commands in PrivExec and Global Config modes

Use this command to display filesystem information.

Syntax

```
show file [information (<FILE>)|systems]
```

Parameters

information <FILE>	Displays information on specified file type
systems	Lists all filesystems

Example

```
RFS7000(config)#show file information flash:
flash::
  type is directory
RFS7000(config)#


RFS7000(config)#show file systems
File Systems:

     Size(B)     Free(B)     Type  Prefix
           -           -   opaque  system:
    10485760     9842688    flash  nvram:
    20971520    20176896    flash  flash:
           -           -  network  (null)
           -           -  network  (null)
           -           -  network  sftp:
           -           -  network  http:
           -           -  network  ftp:
           -           -  network  tftp:
    20971520    20176896        -  hotspot:
RFS7000(config)#
```

2.1.59 password-encryption

Show commands in PrivExec and Global Config modes

Syntax

```
show password-encryption [status]
```

Parameters

status	Displays password encryption status

Example

```
RFS7000#show password-encryption status
Password encryption is disabled
RFS7000#
```

2.1.60 running-config

Show commands in PrivExec and Global Config modes

Displays the contents of the configuration file for the switch, including all configured MAC and IP access lists and access groups applied to an interface.

Syntax

```
show running-config {full|include-factory}
```

Parameters

full	Optional. Displays full configuration
include-factory	Optional. Includes factory defaults

Example

```
RFS7000(config)#show running-config
Warning: This will display secure information.Do you want to proceed? (y/n): y
!
! configuration of RFS7000 version 4.1.2.0-007GD
!
version 1.4
!
!
aaa authentication login default local

no service advanced-vty
!
network-element-id RFS7000
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username "admin" privilege  superuser
username "operator" password 1 40fc8eaf6500a3e4ba113b2be120af8f93b6ae00
!
!
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name

.....................................................................
.....................................................................
RFS7000(config)#
```

2.1.61 securitymgr

Show commands in PrivExec and Global Config modes

Syntax

```
show securitymgr [event-logs]
```

Parameters

event-logs	Displays securitymgr event logs

Example

```
RFS7000#show securitymgr event-logs
RFS7000#
```

2.1.62 sessions

Show commands in PrivExec and Global Config modes

Syntax

```
show sessions
```

Parameters

None

Example

```
RFS7000(config)#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
** 1       cli    172.16.10.10      00:00m      Sep  3 21:55:26 2011
RFS7000(config)#
```

2.1.63 startup-config

Show commands in PrivExec and Global Config modes

Syntax

```
show startup-config
```

Parameters

None

Example

```
RFS7000(config)#show startup-config
Warning: This will display secure information.Do you want to proceed? (y/n): y
!
! configuration of RFS7000 version 4.1.4.0-010GD
!
version 1.4
!
!
aaa authentication login default local

network-element-id RFS7000
!
username "admin" password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username "admin" privilege  superuser
username "operator" password 1 40fc8eaf6500a3e4ba113b2be120af8f93b6ae00
!
!
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
no country-code
logging buffered 4
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
.................................
RFS7000(config)#
```

2.1.64 upgrade-status

Show commands in PrivExec and Global Config modes

Use this command to display last image upgrade status.

Syntax

```
show upgrade-status {detail}
```

Parameters

detail	Optional. Displays detailed last image upgrade log

Example

```
RFS7000#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Sep 03 18:32:17 2011
-------------------------------------------------------
var2 is 10 percent full
/tmp is 5 percent full
Free Memory 151944 kB
FWU invoked via Linux shell
Running from partition /dev/hda6, partition to update is /dev/hda5
Reading image file header
Removing other partition
Added 4.1.0.0-180B *
Making file system
Extracting files (this can take some time).
Version of firmware update file is 4.1.2.0-007GD

Creating LILO files
Running LILO
Added 4.1.0.0-180B *
Added 4.1.0.0-200B
Successful
RFS7000RFS7000#
```

2.1.65 wlan-acl

Show commands common to all modes

Use this command to display WLAN based ACL.

Syntax

```
show wlan-acl [<1-256>|all]
```

Parameters

<1-256>	Displays ACLs attached to a specified WLAN ID. Select the WLAN ID between 1 - 256.
all	Displays all ACLs attached to the WLAN port

Example

```
RFS7000(config)#show wlan-acl 200
WLAN port: 200
  Inbound IP Access List   :
  Inbound MAC Access List  :
  Outbound IP Access List  :
  Outbound MAC Access List :
RFS7000(config)#
```

NOTE The above example applies ACL 110 to a WLAN index 102 in inbound direction.

3

User Exec Commands

Logging in to the switch places you within the USER EXEC command mode. Typically, a log-in requires a user name and a password. You have three attempts to enter a password correctly before a connection attempt is refused.The USER EXEC commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use the **?** at the command prompt. The USER EXEC mode prompt consists of the device host name followed by an angle bracket (**>**). The default host name is generally RFS7000. Use the hostname GLOBAL CONFIG command to change the hostname.

3.1 User Exec Commands

Table 3.1 summarizes User Exec commands.

Table 3.1 User Exec Commands Summary

Command	Description	Ref.
clear	Resets the command to the previous configuration.	*page 3-3*
clrscr	Clears the display screen.	*page 2-2*
cluster-cli	Cluster context.	*page 3-4*
disable	Turns off privileged mode.	*page 3-5*
enable	Turns on privileged mode.	*page 3-6*
exit	Ends the current mode and moves to the previous mode.	*page 2-3*
help	Description of the interactive help system.	*page 2-4*
logout	Exits the EXEC mode.	*page 3-7*
no	Negates a command or sets defaults.	*page 2-6*
page	Toggle paging.	*page 3-8*
ping	Sends ICMP echo messages.	*page 3-8*
quit	Exits the current mode and moves to the previous mode.	*page 3-10*
service	Displays service commands.	*page 2-8*
show	Displays running system information	*page 3-11*
terminal	Displays running system information.	*page 3-14*

Table 3.1 User Exec Commands Summary

Command	Description	Ref.
traceroute	Displays trace route to destination	*page 3-15*

3.1.1 clear

User Exec Commands

Use this command to reset the command to previous configuration.

Syntax

```
clear [crypto-error-log|crypto-log]
```

Parameters

crypto-error-log	Performs clear crypto error log
crypto-log	Perform clear crypto log

Example

```
RFS7000>clear crypto-log
RFS7000>
```

3.1.2 cluster-cli

User Exec Commands

Use this command to cluster all the CLI pertaining to the context it appears. This feature is useful to configure each switch in the cluster by logging in to one switch. This eliminates administrator time and effort N-1 times (if there are N switches in the cluster).

A new context called *redundancy* is created to support cluster-cli. Any commands executed under this context are executed to all members of the cluster.

Syntax

```
cluster-cli [enable]
```

Parameters

enable	Enables cluster context

Usage Guidelines

Enable the redundancy feature before executing this command.

Example

```
RFS7000(config)#show redundancy members

Member ID                     : 192.168.100.1
Member State                  : Peer Seen
Member First Seen             : Nov 15 16:24:54 2011
Member Last  Seen             : Nov 15 16:25:00 2011
Number of HB sent             : 38044
Number of HB received         : 3
Number of Update sent         : 0
Number of Update received     : 0
Member Standby Mode           : Primary
Member AP adoption count      : 0
Member Installed License Count: 0
Member Radio portal Count     : 0
Member Associated MU Count    : 0
Member Rogue AP detected Count: 0
Member Self Healing AP Count  : 0
Member Switch Adopt Capacity  : 0
Member Running Image Version  :

RFS7000(config)#

RFS7000:cluster-cli#show version
*** START: Response from member: 172.20.15.18 ****

RFS7000 version 1.0.0.0-261X
Copyright © 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 7 days, 4 hours 28 minutes

*** END: Response from member: 172.20.15.18 ****

RFS7000 version 1.0.0.0-262X
Copyright © 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 7 days, 4 hours 28 minutes

RFS7000:cluster-cli#
```

3.1.3 disable

User Exec Commands

This command does not do anything in the User Exec mode. The `disable` command is used to exit the PRIV Exec mode. Enable the PRIV mode, then, use the `disable` command to exit the PRIV Exec mode.

Syntax

```
disable
```

Parameters

None

Example

```
RFS7000>enable
RFS7000#

RFS7000#disable
RFS7000>
```

3.1.4 enable

User Exec Commands

Use this command to enter the PRIV mode.

Syntax

```
enable
```

Parameters

None

Example

```
RFS7000>enable
RFS7000#
```

3.1.5 logout

User Exec Commands

Use this command instead of the `exit` command to exit the EXEC mode.

Syntax

```
logout
```

Parameters

None

Example

```
The RFS7000 Series Switch logs off on execution of this command.
```

3.1.6 page

User Exec Commands

Use this command to toggle paging. Enabling this command displays the CLI output page by page, instead of running the entire output at once.

Syntax

```
page
```

Parameters

None

Example

```
RFS7000>page ?
  <cr>

RFS7000>page
```

3.1.7 ping

User Exec Commands

Use this command to send Internet Control Message Protocol's (ICMP) echo packets to network hosts.

Syntax

```
ping [<IP-ADDRESS>|<HOSTNAME>]
```

Parameters

[<IP-ADDRESS>| <HOSTNAME>]	Pings destination address or hostname

Example

```
RFS7000>ping 192.168.235.200
PING 192.168.235.200 (192.168.235.200): 100 data bytes
128 bytes from 192.168.235.200: icmp_seq=0 ttl=128 time=3.8 ms
128 bytes from 192.168.235.200: icmp_seq=1 ttl=128 time=4.3 ms
128 bytes from 192.168.235.200: icmp_seq=2 ttl=128 time=33.0 ms
128 bytes from 192.168.235.200: icmp_seq=3 ttl=128 time=4.0 ms
128 bytes from 192.168.235.200: icmp_seq=4 ttl=128 time=6.5 ms

--- 192.168.235.200 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.8/10.3/33.0 ms
RFS7000>
```

3.1.8 quit

User Exec Commands

Use this command to exit the current mode, and move back to the previous mode.

Syntax

```
quit
```

Parameters

None

Example

In the User Exec mode, the switch logs off upon execution of this command.

3.1.9 show

User Exec Commands

Use this command to exit the current mode and go down to previous mode.

Syntax

```
show <parameter>
```

Parameters

aap-wlan-acl	WLAN based ACL
aap-wlan-acl-stats	IP filtering WLAN based statistics
access-banner	Displays access banner
audit-log-filters	Displays audit log filter rules
autoinstall	Configuration of autoinstall
commands	Displays command lists
crypto	Displays encryption details
crypto-error-log	Displays crypto error log
crypto-log	Displays crypto log
environment	Displays environment information
firewall	Wireless firewall
history	Displays the session command history
interfaces	Displays interface status
ip	Displays the *Internet Protocol* (IP) address
ldap	Displays LDAP server details
licenses	Displays any installed licenses details
logging	Displays the logging configuration and buffer information
mac	Displays MAC access-list assignment
mac-address-table	Displays the MAC address table
mac-name	Displays the configured MAC names
management	Displays L3 Management Interface name
mobility	Displays mobility parameters
ntp	Displays the network time protocol
port	Physical/aggregate port interface
port-channel	Displays port channel commands
privilege	Displays the current privilege level

protocol-list	List of protocols
radius	Displays RADIUS configuration commands.
redundancy	Displays redundancy group parameters
role	Configure role parameters
rtls	*Real Time Locating System* (RTLS) commands
service-list	List of services
smtp-notification	Displays SNMP engine parameters
snmp	Display SNMP engine parameters
snmp-server	Display SNMP engine parameters
spanning-tree	Displays spanning-tree information
static-channel-group	Displays static channel group membership
terminal	Displays terminal configuration parameters
timezone	Displays the timezone
traffic-shape	Displays traffic shaping
users	Displays information about terminal lines
version	Displays the software and hardware version
virtual-ip	IP redundancy feature
wireless	Displays wireless configuration commands
wlan-acl	Displays WLAN based ACL information

Example

```
RFS7000>show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  environment           show environmental information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  port                  Physical/Aggregate port interface
```

```
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  service-list          List of services
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000>

RFS7000>show autoinstall
Warning: This will display secure information.Do you want to proceed? (y/n): y
feature    enabled      URL
config       yes        --not-set--
cluster cfg  yes        --not-set--
image        yes        --not-set--
expected image version  --not-set--
RFS7000>


RFS7000>show history
Warning: This will display secure information.Do you want to proceed? (y/n): y
   1 admin
   2 show
   3 show autoinstall
   4 show autoinstall status
   5 show autoinstall
   6 show history
RFS7000>


RFS7000>show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
RFS7000>
```

3.1.10 terminal

User Exec Commands

Use this command to set the length /number of lines displayed on the terminal window.

Syntax

```
terminal [length <0-512>|no(length <0-512>|width)|width <0-512>]
```

Parameters

length	Sets the number of lines on a screen
no	Negates a command or sets its defaults
width	Sets the width/number of characters on a screen line

Example

```
RFS7000>terminal length 100
RFS7000>

RFS7000>terminal width 200
RFS7000>
```

3.1.11 traceroute

User Exec Commands

Use this command to trace the route to a destination.

Syntax

```
traceroute (<WORD>|IP)
```

Parameters

<WORD>	Traces the route to a destination address or hostname.
IP	IP trace

Example

```
RFS7000>traceroute 192.168.235.200
traceroute to 192.168.235.200 (192.168.235.200), 30 hops max, 38 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
.....................................
.....................................
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
RFS7000>

RFS7000>traceroute 172.16.10.1
traceroute to 172.16.10.1 (172.16.10.1), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  4.581 ms  0.376 ms  0.423 ms
RFS7000>
```

4

Privileged Exec Commands

Most PRIV EXEC mode commands set operating parameters. The PRIV EXEC command set includes those commands contained in the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes using the configure command, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device, followed by a pound sign (**#**). To access PRIV EXEC mode, enter the following command at the prompt:

```
RFS7000> enable
RFS7000#
```

The PRIV EXEC mode is sometimes referred to as **enable mode**, because the `enable` command is used to enter the mode.

4.1 Priv Exec Commands

Table 4.1 summarizes the Priv Exec commands.

Table 4.1 Priv Exec Command Summary

Command	Description	Ref.
acknowledge	Acknowledges alarms	*page 4-3*
archive	Manages archive files	*page 4-4*
change-passwd	Changes the password of the logged in user	*page 4-6*
clear	Resets function	*page 4-7*
clock	Configures the software system clock	*page 4-11*
clrscr	Clears the displayed screen	*page 2-2*
cluster-cli	Cluster context	*page 4-12*
configure	Enters the configuration mode	*page 4-13*
copy	Copies from one file to another	*page 4-14*
disable	Turns off a priviledged mode command	*page 4-15*
enable	Turns on the privileged mode command	*page 4-16*
erase	Erases a filesystem	*page 4-17*
exit	Ends the current mode and moves to the previous mode	*page 2-3*

Table 4.1 Priv Exec Command Summary

Command	Description	Ref.
halt	Halts the switch	*page 4-18*
help	Describes the interactive help system	*page 2-4*
keytransfer	Transfer key for SFTP	*page 4-19*
logout	Exits the EXEC mode	*page 4-20*
no	Negates a command or sets its defaults	*page 2-6*
page	Toggles the paging functionality	*page 4-21*
ping	Sends an ICMP echo message	*page 4-22*
pwd	Displays the current directory	*page 4-23*
quit	Exits the current mode and moves down to the previous mode	*page 4-24*
reload	Halts the switch and performs a warm reboot	*page 4-25*
run	Executes an on-demand self test	*page 4-26*
service	Displays service commands	*page 2-8*
show	Shows system information	*page 4-27*
terminal	Sets terminal line parameters	*page 4-45*
traceroute	Traces a route to a destination	*page 4-46*
upgrade	Upgrades the software image	*page 4-47*
upgrade-abort	Aborts the upgrade process	*page 4-48*
write	Writes the running configuration to memory or terminal	*page 4-49*

4.1.1 acknowledge

Priv Exec Commands

Use this command to acknowledge alarms.

Syntax

```
acknowledge alarm-log [<1-65535>|all]
```

Parameters

alarm-log	Acknowledges alarms
<1-65535>	Acknowledges a specified alarm. Select the alarm ID between 1 - 65535.
all	Acknowledges all alarms

Example

```
RFS7000#acknowledge alarm-log all
RFS7000#
```

4.1.2 archive

Priv Exec Commands

Use this command to manage archive files.

Syntax

```
archive tar [/table|/create|/xtract]

archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] <FILE>
archive tar /xtract [<FILE>|<URL>] <DIR>
```

Parameters

tar	Manipulates (creates, lists or extracts) a tar file • /table – Lists files in a tar file • /create – Creates a tar file • /xtract – Extracts files from a tar file
<FILE>	Tar filename. The file can exist in: • flash://path/file • nvram:startup-config • system:running-config
<URL>	Tar file URL. The file can exist in: • sftp://<user>@<hostname|IP>[:port]/path/file

Example

```
RFS7000#archive tar /create ?
  FILE  Tar filename
        Files: flash:/path/file
               nvram:startup-config
  URL   Tar file URL
        URLs:  sftp://<user>@<hostname|IP>[:port]/path/file
RFS7000#

RFS7000#archive tar /table ?
  FILE  Tar filename
        Files: flash:/path/file
               nvram:startup-config
               system:running-config
  URL   Tar file URL
        URLs:  sftp://<user>@<hostname|IP>[:port]/path/file
RFS7000#

RFS7000#archive tar /xtract ?
  FILE  Tar filename
        Files: flash:/path/file
               nvram:startup-config
               system:running-config
  URL   Tar file URL
        URLs:  sftp://<user>@<hostname|IP>[:port]/path/file
RFS7000#
```

How to zip the folder flash:/log/?

```
RFS7000#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
RFS7000#dir flash:/
```

Viewing the output tar file?

```
Directory of flash:/
  drwx   1024      Thu Aug 17 08:25:50 2006   hotspot
  drwx   120       Fri Sep  8 12:27:20 2006   log
  drwx   1024      Thu Sep  7 16:23:34 2006   crashinfo
  drwx   1024      Wed Aug 23 15:30:19 2006   backup
  -rw-   173056    Fri Sep  8 14:39:48 2006   out.tar
```

Which files are tared?

```
RFS7000#archive tar /table flash:/out.tar
drwxrwxrwt 0/600         0 2006-09-08 12:27:20 flash/log
-rw-r--r-- 0/0         381 2006-09-08 12:27:28 flash/log/snmpd.log
-rw-r--r-- 0/0      151327 2006-09-08 14:37:26 flash/log/messages.log
-rw-r--r-- 0/0       17318 2006-09-08 12:27:29 flash/log/startup.log
drwxrwxrwt 0/600         0 2006-09-08 12:27:14 flash/log/radius
```

Untar fails..?

```
RFS7000#archive tar /xtract flash:/out.tar flash:/out/
tar: flash:/out.tar: No such file or directory
```

4.1.3 change-passwd

Priv Exec Commands

Use this command to change the password of the logged in user.

Syntax

```
change-passwd
```

Parameters

None

Usage Guidelines

A password must be between 8 to 32 characters in length. For safety, the console does not display the user entered key words (refer example) for the `old password` and `new password` fields.

Ensure the console displays the password successfully changed message.

NOTE The console, by default, does not display any user entered keyword for the old pasword and new password fields.

Leaving the `old password` and `new password` fields empty displays the following error message:
`Error: Invalid password length. It should be between 8 - 32 characters.`

Example

```
RFS7000#change-passwd
Enter old password:
Enter new password:
Re Enter new password:
% Error:Invalid password length. It should be between 8 and 32 characters
RFS7000#


RFS7000#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
RFS7000#
```

4.1.4 clear

Priv Exec Commands

Use this command to reset the current context.

Syntax

```
clear [aclstats|alarm-log|arp-cache|counters|crypto|crypto-error-log|crypto-log|
  dosstats|ip|logging|mac-address-table|mobility|remote-login-lock|spanning-tree]

clear alarm-log [<1-65535>|acknowledge|all|new]

clear counters [all|bridge|firewall|igmp-snooping|interface|router|thread]
clear counters interface [<IFNAME>|all|ge <1-4>|me1|sa <1-4>|vlan <1-4094>|
router|thread]

clear crypto [ipsec|isakmp] [sa] [<Peer-IP-address>]

clear ip [dhcp|pmtu-discovery-blackhole-cache]
clear ip dhcp [binding] [*|<A.B.C.D>|all]

clear mac-address-table [dynamic|multicast|static] [address|
  bridge <1-32>|interface|vlan <1-4094>]

clear mobility [event-log|mobile-unit|peer-statistics]
clear mobility event-log (mobile-unit|peer)
clear mobility mobile-unit [<AA-BB-CC-DD-EE-FF>|all|foreign-database|home-database]
clear mobility peer-statistics <Peer-IP-Address>

clear remote-login-lock [gui|ssh]

clear spanning-tree [detected-protocols] {interface(<IFNAME>)}
```

Parameters

clear (aclstats)	
aclstats	Clears *Access Control List* (ACL) statistics
clear (alarm-log)	
alarm-log [<1-65535>| acknowledge| all|new]	Clears alarm logs based on the option selected • <1-65535> – Clears a specified alarm. Specify the alarm ID between 1 - 65535. • acknowledge – Clears acknowledged alarms • all – Clears all alarms • new – Clears new alarms
clear (arp-cache)	
arp-cache	Clears the *Address Resolution Protocol* (ARP) cache

clear (counters)	

counters [all|bridge|interface| firewall|igmp-snooping| router|thread]	Clears counters
	• all – Clears all counters
	• bridge – Clears bridge counters
	• interface [<IFNAME>|all|ge|me1|sa|vlan] – Clears interface counters
	  • <IFNAME> – Clears specified interface counters. Specify the interface name to clear counters
	  • all – Clears all interface counters
	  • ge <1-4> – Clears specified Gigabit Ethernet interface counters. Specify the interface index between 1 - 4.
	  • me1 – Clears all Fast Ethernet interface counters
	  • sa <1-4> – Clears specified Static Aggregate interface counters. Specify the interface index between 1 - 4.
	  • vlan <1-4094> – Clears specified VLAN interface counters. Specify the interface ID between 1 - 4094.
	• firewall - Clears firewall counters
	• igmp-snooping - Clears IGMP snooping counters
	• router – Clears router counters
	• thread – Clears per-thread counters

clear (crypto)	

crypto [ipsec|isakmp] (sa) <PEER-IP-ADDRESS>	Clears encryption subsystem
	• ipsec (sa) – Flushes *IP Security* (IPSec) *security associations* (SA) for a specified peer
	  • <PEER-IP-ADDRESS> – Specify the peers's *Internet Protocol* (IP) address.
	• isakmp (sa) – Flushes the *Internet Security Association and Key Management Protocol* (ISAKMP) *Internet Key Exchange* (IKE) SAs for a specified pee.
	  • <PEER-IP-ADDRESS> – Specify the peer's IP address.

clear (crypto-error-log)	
crypto-error-log	Clears crypto error logs
clear (crypto-log)	
crypto-log	Clears crypto log
clear (dosstats)	
dosstats	Clears DOS statistics

clear (ip)	

ip [dhcp|pmtu-discovery-blackhole-cache]	Clears the IP *Dynamic Host Configuration Protocol* (DHCP) server settings
	• dhcp – Clears DHCP server configuration
	  • bindings – Clears DHCP server address bindings based on the option selected
	  • * – Clears all bindings
	  • A.B.C.D – Clears specific bindings. Specify the IP address to clear associated bindings
	  • all – Clears all bindings
	• pmtu-discovery-blackhole-cache - Clears path-MTU discovery blackhole cache

clear (logging)	
logging	Modifies message logging facilities
clear (mac-address-table)	

mac-address-table [dynamic|multicast|static]	Clears all entries in the forwarding database (Layer2 MAC entries)
	• dynamic – Clears all dynamic entries
	• multicast – Clears all multicast entries
	• static – Clears all entries configured through management
	The following are common to all of the above parameters:
	  • address – Clears the specified MAC Address/ Interface Name/ VLAN ID (1-4094)
	  • bridge <1-32> – Clears the specified bridge group for bridging. Specify the bridge group index between 1- 32.
	  • interface – Clears MAC address for the specified interface. Specify the MAC Address/ Interface Name/ VLAN ID (1-4094).
	  • vlan – Clears MAC address for the specified VLAN interface. Specify the MAC Address/ Interface Name/ VLAN ID (1-4094).

clear (mobility)	

mobility
[event-log|
mobile-unit|
peer-statistics]
	Clears mobility attributes
	• event-log – Clears all event logs based on the option selected
	  • mobile-unit – CLears mobile unit event logs
	  • peer – Clears peer event logs
	• mobile-unit – Clears a mobile unit
	  • <AA-BB-CC-DD-EE-FF> – Clears a specified mobile unit. Specify the MAC address of the mobile unitall – Clears all mobile units (home and foreign)
	  • foreign-database – Clears mobile units present in the foreign mobile unit database
	  • home-database – Clears mobile units present in the home mobile unit database
	• peer-statistics – Clears mobility peer statistics
	  • <Peer-IP-Address> – Clears mobility statistics for a specified peer. Specify the IP address of the peer. Clears all peer statistics if no peer is specified

clear (remote-login-lock)	
remote-login-lock [gui|ssh]	Clears remote login lock based on the option selected • gui – Removes Web UI lock • ssh – Removes *Secure Shell* (SSH) lock. The lock can be removed through console management interface (local RS-232 port) only.
clear (spanning-tree)	

spanning-tree
[detected-protocols]
{interface <IFNAME>}
	Clears spanning tree attributes
	• detected-protocols – Clears spanning tree detected protocols
	  • interface – Clears detected protocols for a specified interface
	  • <IFNAME> – Specify the interface name. Clears spanning tree attributes for all interfaces, if no interface name is specified

Example

```
RFS7000#clear spanning-tree detected-protocols
RFS7000#

RFS7000#clear arp-cache
RFS7000#
```

4.1.5 clock

Priv Exec Commands

Use this command to configure the software system clock.

Syntax

```
clock set HH:MM:SS [1-31] MONTH [1993-2035]
```

Parameters

set	Sets the system date and time

Example

```
RFS7000#clock ?
  set  Set system date & time

RFS7000#clock set ?
  HH:MM:SS  Current Time (in military format hours, minutes and seconds)

RFS7000#clock set 12:45:01 ?
  <1-31>  Day of the month

RFS7000#clock set 12:45:01 14 ?
  MONTH  Month of the year (Jan to Dec)

RFS7000#clock set 12:45:01 14 Oct ?
  <1993-2035>  Valid 4 digit year

RFS7000#clock set 12:45:01 14 Oct 2011 ?
  <cr>

RFS7000#clock set 12:45:01 14 Oct 2011
RFS7000#show clock
Oct 14 12:45:07 UTC 2011
RFS7000#
```

4.1.6 cluster-cli

Priv Exec Commands

Use this command to cluster all the CLI pertaining to the context it appears. This feature is useful to configure each switch in the cluster by logging in to one participating switch. This eliminates administrator time and effort, as one switch configuration can represent the entire cluster.

A new context called *redundancy* is available to support the cluster-cli. Any commands executed under this context are also executed in each cluster member.

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the cluster context

Example

```
RFS7000(config)#show redundancy-members

Member ID                     : 192.168.100.1
Member State                  : Peer Seen
Member First Seen             : Mar 15 16:24:54 2008
Member Last  Seen             : Mar 15 16:25:00 2008
Number of HB sent             : 38044
Number of HB received         : 3
Number of Update sent         : 0
Number of Update received     : 0
Member Standby Mode           : Primary
Member AP adoption count      : 0
Member Installed License Count: 0
Member Radio portal Count     : 0
Member Associated MU Count    : 0
Member Rogue AP detected Count: 0
Member Self Healing AP Count  : 0
Member Switch Adopt Capacity  : 0
Member Running Image Version  :

RFS7000(config)#
```

4.1.7 configure

Priv Exec Commands

Use this command to move into the global configuration mode.

Syntax

```
configure terminal
```

Parameters

terminal	Configures from the terminal

Example

```
RFS7000#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RFS7000(config)#
```

4.1.8 copy

Priv Exec Commands

Use this command to copy any file (config, log, txt...etc) to and from the switch.

NOTE Copying a new config file onto an existing running-config file merges it with the existing running-config. Both, the existing running-config and the new config file are applied as the current running-config of the switch.

Copying a new config file onto a start-up config file replaces the existing start-up config file with the parameters of the new config file. It is always better to erase the existing start-up file from the switch and then copy the new config to the startup config.

Syntax

```
copy (FILE|URL) (FILE|URL)
```

Parameters

FILE	Target file from which to copy. Select from: • flash:/path/file • nvram:startup-config • system:running-config
URL	The target URL from which to copy. Select from: • sftp://<user>@<hostname:port or IP>/path/file

Example

```
RFS7000#copy ?
  FILE  File from which to copy
        Files: flash:/path/file
               nvram:startup-config
               system:running-config
  URL   URL from which to copy
        URLs: sftp://<user>@<hostname:port or IP>/path/file

RFS7000#copy
```

Transferring file snmpd.log to remote tftp server?

```
RFS7000#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switchrunning-config?

```
RFS7000#copy tftp://157.235.208.105:/running-
config running-config
```

4.1.9 disable

Priv Exec Commands

Use this command to exit the Priv Exec mode and move to the User Exec mode.

Syntax

```
disable
```

Parameters

None

Example

```
RFS7000#disable
RFS7000>
```

4.1.10 enable

Priv Exec Commands

Use this command to move from the User Exec mode to the Priv Exec mode. It turns on the privileged mode command. This command does not do anything in the Priv Exec mode.

Syntax

```
enable
```

Parameters

None

Example

```
RFS7000>enable
RFS7000#
```

4.1.11 erase

Priv Exec Commands

Use this command to erase a target filesystem.

Syntax

```
erase startup-config
```

Parameters

startup-config	Resets the switch configuration to factory default settings

Example

```
RFS7000#erase ?
startup-config  Reset configuration to factory default
```

4.1.12 halt

Priv Exec Commands

Use this command to halt the switch. This command is similar to the `reload` command. The only difference is that `halt` command stops the switch and `reload` stops and restarts the switch.

Syntax

```
halt
```

Parameters

None

Example

```
RFS7000#halt
Wireless switch will be halted, do you want to continue? ([y]es/[n]o): n
RFS7000#
```

4.1.13 keytransfer

Priv Exec Commands

Use this command to transfer keys for *Secure File Transfer Protocol* (SFTP).

Syntax

```
keytransfer host <IPADDR> user <WORD>
```

Parameters

keytransfer	Transfers keys for the *Secure File Transfer Protocol* (SFTP) server. Public key must be transferred between RFS7000 and SFTP server via CLI before making a SFTP communication.
host <Host-IP-Address>	Sets the IP address of the SFTP server in the A.B.C.D format
user <WORD>	Configures user access to the SFTP server. Specify the name of the user to provide access

Example

```
RFS7000#keytransfer host 157.235.208.252 user motorola1

ssh keygen for cli in progress
Transfer of ssh public key in progress: for CLI
ssh: connect to host 157.235.208.252 port 22: Network is unreachable
RFS7000#
```

4.1.14 logout

Priv Exec Commands

Use this command to exit the EXEC mode.

Syntax

```
logout
```

Parameters

None

Example

```
RFS7000#logout
Please press Enter to activate this console.
```

4.1.15 page

Priv Exec Commands

Use this command to toggle switch paging. Enabling this command displays the command output page by page, instead of running the entire output at once.

Syntax

```
page
```

Parameters

None

Example

```
RFS7000#page
RFS7000#show running-config
Warning: This will display secure information.Do you want to proceed? (y/n): y
!
! configuration of RFS7000 version 4.1.2.0-007GD
!
version 1.4
!
!
aaa authentication login default local

no service advanced-vty
!
network-element-id RFS7000
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username "admin" privilege  superuser
username "operator" password 1 40fc8eaf6500a3e4ba113b2be120af8f93b6ae00
!
!
!
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
```

4.1.16 ping

Priv Exec Commands

Use this command to send *Internet Control Message Protocol's* (ICMP) echo packets to network hosts.

Syntax

```
ping [<WORD>]
```

Parameters

<WORD>	Specify the destination address or hostname to ping

Example

```
RFS7000#ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10): 100 data bytes
128 bytes from 172.16.10.10: icmp_seq=0 ttl=128 time=1.4 ms
128 bytes from 172.16.10.10: icmp_seq=1 ttl=128 time=0.6 ms
128 bytes from 172.16.10.10: icmp_seq=2 ttl=128 time=0.5 ms
128 bytes from 172.16.10.10: icmp_seq=3 ttl=128 time=0.5 ms
128 bytes from 172.16.10.10: icmp_seq=4 ttl=128 time=0.3 ms

--- 172.16.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.6/1.4 ms
RFS7000#
```

4.1.17 pwd

Priv Exec Commands

Use this command to view the contents of the present working directory.

Syntax

```
pwd
```

Parameters

None

Example

```
RFS7000#pwd
flash:/
RFS7000#
```

4.1.18 quit

Priv Exec Commands

In the Priv Exec mode, use this command to quit current session, without saving changes, and shut down the switch.

Syntax

```
quit
```

Parameters

None

Example

```
RFS7000#quit

RFS7000 version 1.0.0.0-016GR
Login as 'cli' to access CLI.
RFS7000 login:
```

4.1.19 reload

Priv Exec Commands

Use this command to halt the switch and perform a warm reboot.

Syntax

```
reload
```

Parameters

None

Example

```
RFS7000#reload
Wireless switch will be rebooted, do you want to continue? (y/n): y

RFS7000 login:
```

4.1.20 run

Priv Exec Commands

Use this command to execute a self test.

Syntax

```
run [self-test]
```

Parameters

self-test	Performs an on-demand self-test

Example

```
RFS7000#run self-test
Self test started
FIPS Power-On Self Test started
Fri Oct 14 15:10:50 2011   FIPS self test started this can take some time
Fri Oct 14 15:10:54 2011   FIPS integrity check of the WIOS image successful
Fri Oct 14 15:10:54 2011   FIPS data integrity check is successful
Fri Oct 14 15:10:54 2011   FIPS power-up tests for openSSL library
Fri Oct 14 15:10:55 2011   1. Automatic power-up self test includes RNG, HMAC, AES,
3DES, RSA selftests...Successful
Fri Oct 14 15:10:55 2011   2. AES encryption/decryption...Successful
Fri Oct 14 15:10:56 2011   3. RSA key generation and encryption/decryption...successful
Fri Oct 14 15:10:56 2011   4. 3DES-ECB encryption/decryption...successful
Fri Oct 14 15:10:56 2011   5a. SHA-1 hash...successful
Fri Oct 14 15:10:56 2011   5b. SHA-256 hash...successful
Fri Oct 14 15:10:56 2011   5c. SHA-512 hash...successful
Fri Oct 14 15:10:56 2011   5d. HMAC-SHA-1 hash...successful
Fri Oct 14 15:10:56 2011   5e. HMAC-SHA-224 hash...successful
Fri Oct 14 15:10:56 2011   5f. HMAC-SHA-256 hash...successful
Fri Oct 14 15:10:56 2011   5g. HMAC-SHA-384 hash...successful
Fri Oct 14 15:10:56 2011   5h. HMAC-SHA-512 hash...successful
Fri Oct 14 15:10:56 2011   The tests completed without errors
Fri Oct 14 15:10:56 2011   openSSL power-up self test successful
Fri Oct 14 15:10:56 2011   FIPS power-up tests for quickSec library
Power-up test for Quicksec library
==[Random number test]=============================================================
  1. `ansi-x9.31' (test_random) ... ok
==[Hash test]======================================================================
  2. `SHA test' (hash_static_tests) ... ok
==[MAC tests]======================================================================
  3. `HMAC-SHA test' (mac_static_tests) ... ok
==[Cipher tests]===================================================================
  4. `AES & 3DES test' (cipher_static_tests) ... ok

no errors encountered.
Fri Oct 14 15:10:56 2011   quickSec power-up self test successful
Fri Oct 14 15:10:56 2011   FIPS power-up tests for user space wireless crypto library
Fri Oct 14 15:10:56 2011   User space wireless crypto self test for AES-CBC successful.
Fri Oct 14 15:10:56 2011   User space wireless crypto self test successful
Fri Oct 14 15:10:56 2011   Starting XLR crypto test
Fri Oct 14 15:10:56 2011   AES test successful...
Fri Oct 14 15:10:56 2011   TDES test successful...
Fri Oct 14 15:10:56 2011   SHA1 test successful...
Fri Oct 14 15:10:56 2011   SHA256 test successful...
Fri Oct 14 15:10:56 2011   Successfully completed XLR crypto test
Self test completed
RFS7000#
```

4.1.21 show

Priv Exec Commands

Use this command to show currently running system information.

Syntax

```
show <display parameter>
```

Parameters

aap-wlan-acl [<1-256>|all]	Displays WLAN based ACL • <1-256> – The WLAN ID (this displays the ACL attached to the WLAN ID specified by the <1-256> value) • all – Displays all ACLs attached to WLAN port
aap-wlan-acl-stats	Displays IP filtering WLAN based statistics
access-banner	Displays the access banner
access-list {<1-99>|<100-199>| <1300-1999>| <2000-2699>] <WORD>}	Displays access list details based on the option selected. The options are: • <1-99> – IP standard access list • <100-199> – IP extended access list • <1300-1999> – IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <WORD> – Specify the access list name to view details.

aclstats [access-list|vlan]	Displays ACL statistics
	• access-list {<1-99>| <100-199>| <1300-1999>|<2000-2699>|<WORD>} – Displays access list configuration.
	  • <1-99> – Optional. IP standard access list
	  • <100-199> – Optional. IP extended access list
	  • <1300-1999> – Optional. IP standard access list (expanded range)
	  • <2000-2699> – Optional. IP extended access list (expanded range)
	  • <WORD> – Optional. Specify the access list name to view statistics.
	• vlan [<1-4094>] – Displays ACL configuration for a specified VLAN interface
	  • <1-4094> – Specify the VLAN ID between 1 - 4094.

alarm-log {<1-65535>| acknowledged| all|count|new| severity-to-limit}	Displays all alarms currently in the system.
	• <1-65535> – Optional. Displays details of specified alarm. Specify the alarm ID between 1 - 65535.
	• acknowledged – Optional. Displays acknowledged alarms currently in the system
	• all – Optional. Displays all alarms currently in the system
	• count – Displays count of alarms currently in the system
	• new – Optional. Displays new alarms currently in the system
	• severity-to-limit {critical|informational|major|normal|warning} – Optional. Displays all alarms with specified or higher severity level. The alarm severity levels are:
	  • critical – Optional. Displays all critical alarms
	  • informational – Optional. Displays all informational or higher severity alarms
	  • major – Optional. Displays all major or higher severity alarms
	  • normal – Optional. Displays all normal or higher severity alarms
	  • warning – Optional. Displays all warning or higher severity alarms

audit-log-filters	Displays audit log filter rules
autoinstall {status}	Displays autoinstall configuration • status – Optional. Displays autoinstall status (whether initiated or not)
boot	Displays the boot configuration
clock	Displays the system clock
commands	Lists all ‘show’ command parameters

crypto
[ipsec|isakmp|
key|map|
pki]
	Displays encryption related commands
	• ipsec [sa|security-associaton|transformset] – Displays IPSEC policy details
	  • sa – Displays IPsec *security associations* (SAs)
	  • security-association (lifetime) – Displays lifetime SAs
	  • transformset {<WORD>} – Displays a specified transformset. The system displays all transformsets, if no transformset name is specified.
	• isakmp [policy|sa] – Displays ISAKMP policy details
	  • policy {<1-10000>} -— Optional. Displays ISAKMP policy of the sequence number <1-10000> value
	  • sa – Displays all crypto ISAKMP SAs
	• key [mypubkey] – Displays authentication key management
	  • mypubkey [rsa] – Displays public keys associated with the switch
	  • rsa – Displays *Rivest, Shamir, and Adleman* (RSA) public keys
	• map {interface|tag} – Displays crypto map details
	  • interface <WORD> – Optional. Displays crypto maps for a specified interface
	  • <WORD> – Specify the interface name.
	  • tag <WORD> – Optional. Displays crypto maps with a specified tag
	  • <WORD> – Specify the crypto map name.
	• pki [request|trustpoints] – Display*s Public Key Infrastructure* (pki) commands
	  • request <WORD> – Displays certificate request
	  • <WORD> – Specify the trustpoint name to view certificate request.
	  • trustpoints – Displays configured trustpoints configuration details

crypto-error-log	Displays crypto error log
crypto-log	Displays crypto log
debugging mstp	Displays debugging information outputs • mstp – Displays *Mutiple Spanning Tree Protocol* (MSTP) debugging status
dhcp [config|status]	Displays the DHCP server configuration and status • config – Displays DHCP server configuration • status – Displays DHCP server status (running or not)
environment	Displays environmental information

firewall [config|dhcp|flow]	Displays wireless firewall
	• config – Displays firewall configuration details
	• dhcp [snoop-table] – DHCP based firewalls
	  • snoop-table – Displays snoop table entries
	• flow (timeouts) – Displays firewall flows
	  • timeouts – Displays wireless firewall flow timeout configuration

history	Displays session command history
interfaces {<IFNAME>| ge <1-4>|me1| sa <1-4>|switchport| vlan <1-4094>}	Displays interface status. Select the interface type to view status. • <IFMNAME> – Optional. Displays the specified interface status. Specify the interface name • ge1 <1-4> –Optional. Displays the specified GigabitEthernet interface status. Select the interface index between 1 - 4. • me1 – Optional. Displays FastEtherner interface status • sa <1-4> – Optional. Displays the specified StaticAggregate interface status. Select the interface index between 1 - 4. • switchport [<IFNAME>|ge <1-4>|me1|sa <1-4>|vlan <1-4094>] – Optional. Displays status of the layer 2 interfaces. Specify the interface type to view status. • vlan <1-4094> – Optional. Displays the specified VLAN interface status. Select the interface index between 1 - 4094. If no interface name or type is specified, the system displays status of all interfaces configured,

ip [access-group|
access-list|arp|ddns|
dhcp|
dhcp-vendor-options|
domain-name|dos|
http|igmp|interface|
name-server|nat|route|
routing|ssh]
	Displays IP configuration
	• access-group [<IFNAME>|all|ge <1-4>|me1|role <ROLE-NAME>|
	sa <1-4>|vlan <1-4094>] – Displays ACLs. attached to an interface
	  • <IFNAME> – The interface to display access-group information for.
	  • all – Displays access-group information for all interfaces
	  • ge <1-4> – Displays access-group information for the GigabitEthernet interface specified by <1-4> value
	  • me1 – Displays access-group information for the FastEthernet interface
	  • role <ROLE-NAME> – Displays access-group information for the role. specified by the <ROLE-NAME> value
	  • sa <1-4> – Displays access-group information for the StaticAggregate. interface specified by <1-4> value
	  • vlan <1-4094> – Displays access-group information for the VLAN specified by the <1-4094> value
	• access-list – Lists *Internet Protocol* (IP) access control lists
	• arp – Displays ARP related configuration
	• ddns – Displays *Dynamic Domain Name System* (DDNS) configuration
	  • binding – Displays DNS address bindings
	• dhcp [binding|class|pool|sharednetwork] – Displays DHCP server configuration
	  • binding {manual} – Displays all DHCP address bindings. Specify 'manual' to view static DHCP address bindings
	  • class {NAME} – Displays DHCP server classes. Specify the class name to view details of a specified class
	  • pool {NAME} – Displays DHCP pools. Specify the pool name to view details of a specified pool
	  • sharednetwork – Displays DHCP shared networks

	• dhcp-vendor-options – Displays DHCP option 43 parameters received from the DHCP server
	• domain-name – Displays default domain for the DNS server
	• dos [config|stats] – Displays *Denial of Service* (DOS) configuration
	  • config – Displays IP DOS configuration
	  • stats – Displays IP DOS statistics
	• http [secure-server] – Displays *HyperText Transfer Protocol Secure* (HTTPS) status
	  • secure-server – Displays if HHTPS server is running or not. Also displays the HHTPS server configuration status and the trustpoint used
	• igmp [snooping] – Displays the *Internet Group Management Protocol* (IGMP) configuration
	  • snooping {mrouter|querier|vlan} – Displays the IGMP snooping configuration
	  • mrouter – Optional. Displays multicast router configuration
	  • querier – Optional. Displays IGMP querier configuration
	  • vlan – Optional. Identifies the VLAN in use
	• interface {<IFNAME>|brief|vlan} – Displays interface IP information.
	  • <IFNAME> {brief} – Optional. Displays brief IP status and configuration summary for a specified interface. Specify the interface name to view summary.
	  • brief – Optional. Displays brief IP status and configuration summary of all configured interfaces
	  • vlan <1-4094> {brief} – Optional. Displays brief IP status and configuration summary for a specified VLAN interface. Specify the VLAN interface index between 1 - 4094 to view summary.
	• name-server – Displays the IP configuration of DNS name servers

	• nat [interfaces|translations] – Displays *Network Address Translations* (NAT) configuration
	  • interfaces – Displays NAT configuration on interfaces
	  • translations {inside|outside|verbose} – Displays NAT translations.
	  • Inside [destination|source] – Optional. Displays inside destination/source NAT translations
	  • Outside [destination|source] – Optional. Displays outside destination/source NAT translations
	  • verbose – Optional. Displays NAT translations in real time
	• route {A.B.C.D|A.B,C.D/M|detail} – Displays IP routing table
	  • A.B.C.D – Optional. Specifies the network in the IP routing table to display
	  • A.B.C.D/M – Optional. Specifies IP prefix <network> <length> (for example, 35.0.0.0/8)
	  • detail – Optional. Displays all IP routing tables in detail
	• routing – Displays routing status
	• ssh – Displays SSH server status and configuration

ldap configuration {primary|secondary}	Displays *Lightweight Directory Access Protocol* (LDAP) server data
	• configuration {primary|secondary} – Displays following LDAP server configuration parameters:
	  • primary – Optional. Displays primary LDAP server configuration
	  • secondary – Optional. Displays secondary LDAP server configuration

licenses	Displays installed license details
logging	Displays logging configuration and buffer
mac [access-group| access-list]	Displays MAC access-list assignment details • access-group [<IFNAME>|all|ge <1-4>|me1|role <ROLE-NAME>| sa <1-4>|vlan <1-4094>] – Displays MAC ACLs attached to an ineterface. Specify the interface type and interface name or index to view access group attached to a specific interface. • access-list – Lists all MAC access lists
mac-address-table	Displays MAC address table
mac-name	Displays the configured MAC names
management	Displays L3 management interface details

mobility [event-log|forwarding|global|mobile-unit|peer|statistics]	Displays following mobility parameters:
	• event-log [mobile-unit|peer] – Displays event logs
	  • mobile – Displays station event logs
	  • peer – Displays peer event logs
	• forwarding {<AA-BB-CC-DD-EE-FF>} – Displays mobile units in the forwarding plane
	  • <AA-BB-CC-DD-EE-FF> – Optional. To view a specific mobile unit in the forwarding plane, specify the MAC address of the mobile unit.
	• global – Displays global mobility parameters
	• mobile-unit {<AA-BB-CC-DD-EE-FF>|detail} – Displays mobile-units in the mobility database
	  • <AA-BB-CC-DD-EE-FF> – Optional. To view a specific mobile unit in the mobility database, specify the MAC address of the mobile unit.
	  • detail – Optional. Displays detailed information
	• peer {<A.B.C.D>|detail} – Displays mobility peers
	  • <A.B.C.D> – To view a specific mobility peer, specify the IP address of the peer.
	  • detail – Displays detailed information
	• Statistics {<AA-BB-CC-DD-EE-FF>} – Displays mobility statistics
	  • <AA-BB-CC-DD-EE-FF> – Optional. To view mobility statistics of a specified mobile unit, specify the MAC address of the mobile unit.

ntp [associations|status]	Displays *Network Time Protocol* (NTP) configuration • associations {detail} – Displays NTP associations • detail – Displays NTP association details • status – Displays NTP status
password-encryption status	Displays password encryption status (whether enabled or not)
port fw config	Displays Physical/Aggregate port interface • fw config – Displays configurable firewall parameters
port-channel load-balance	Displays port channel load balancing
privilege	Displays the current privilege level
protocol-list	Lists all protocols

radius [configuration|eap| group|nas|proxy| rad-user| trust-point]	Displays RADIUS configuration commands • configuration – Displays RADIUS server configuration (status and data source) • eap [configuration] – Displays RADIUS *Extensible Authentication Protocol* (EAP) configuration. *EAP-Transport Layer Security* (EAP-TLS) is enabled by default • group {<WORD>} – Displays RADIUS groups in the local database. To view a specific RADIUS group, specify the group name. • nas {<A.B.C.D/M>} – Displays all client information. To view a specific client information. specify the IP address and mask of the client. • proxy {<WORD>} – Displays proxy information. To view a specific proxy information. specify the proxy realm name. • rad-user {<WORD>} – Displays RADIUS user (users existing in the local RADIUS database) information. To view a specific RADIUS user information. specify the user name. • trust-point – Displays RADIUS trustpoint configuration

redundancy-group
[dynamic-ap-load-balance|
group|history|
members]
	Displays redundancy group parameters.
	• dynamic-ap-load-balance [config] – Displays redundancy dynamic AP load balance configuration
	• group {config|runtime} – Displays redundancy group configuration
	  • config – Displays redundancy group configuration information
	  • runtime – Displays redundancy group runtime information
	• history – Displays state transition history of the switch
	• members {<A.B.C.D>|brief} – Displays redundancy group members in detail
	  • <A.B.C.D> – Optional. Specify member IP address, to view details of a specific group member.
	  • brief – Optional. Displays all members in brief

role {<WORD>|mobile-units}	Displays following role parameters: • <WORD> – Displays a specific role details. Specify the role name. If no role is specified, the system displays all configured roles. • mobile-units – Displays mobile-units assigned with these roles

rtls [aeroscout|ekahau|filter|site|sole|tags|zone]	Displays following *real time locating system* (RTLS) parameters:
	• aeroscout – Displays AeroScout configurations
	• ekahau – Displays ekahau configurations
	• filter {<1-100>} – Displays *Radio Frequency Identification* (RFID) tag filters. To view a specific tag filter, select the tag index between 1 - 100.
	• site – Displays site configurations
	• sole [peers|probes] – Displays following SOLE configuration:
	  • peers – Displays SOLE peer information
	  • probes – Displays SOLE probe information
	• tags {aeroscout|all|ekahau|g2|mobile-unit|rfid|zone} – Displays tags/assets (passive/active/wi-fi) information, based on the option selected
	  • aeroscout {all} – Displays all located aeroscout tags
	  • all – Displays all tags
	  • ekahau {all} – Displays all located ekahau tags
	  • g2 {all} – Displays all located G2 tags
	  • mobile-unit {all} – Displays all located mobile units (802.11 clients)
	  • rfgid {all} – Displays all located RFID gen2 tags
	  • zone <1-48> – Displays zone configuration. Select the zone index between 1 - 48
	• zone {<1-48>|detail} – Displays zone statistics
	  • <1-48> – Optional. Displays statistics for the zone specified by the <1-48> value
	  • detail – Displays zone details

running-config {full|include-factory}	Displays the current operating configuration • full – Optional. Displays full configuration • include-factory – Optional. Includes factory defaults
securitymgr eventlogs	Displays securitymgr event logs
service-list	Lists all available services
smtp-notification {traps}	Displays *Simple Network Management Protocol* (SNMP) engine configuration • traps – Displays SNMP trap enable/disable flags

snmp user [snmpmanager|snmpoperator|snmptrap]	Displays SNMP engine user types
	• user [snmpmanager|snmpoperator|snmptrap] – Select the SNMP user to display information for.
	  • snmpmanager – Displays manager information
	  • snmpoperator – Displays operator information
	  • snmptrap – Displays trap information

snmp-server {traps}	Displays SNMP server configuration • traps – Displays trap enable flags
spanning-tree mst {configuration|detail|instance}	Displays spanning tree information. • mst {configuration|detail|instance} – Displays MST information • configuration – Displays MST configuration information • detail interface [<IFNAME>|ge <1-4>|me1|sa <1-4>|vlan <1-4094>] – Displays MST detailed information. To view MST detailed information for an interface, specify the interface type and name/index. • instance <1-15> – Displays MST information for an interface instance. Select the interface instance index between 1 - 15.
startup-config	Displays the startup configuration
static-channel-group	Displays static channel group membership
terminal	Displays terminal configuration
timezone	Displays the timezone setting defined for the switch
traffic-shape [config| priority-map|statistics]	Displays traffic shaping information based on the option selected • config {class <1-4>} – Displays traffic class shaping configuration. Maximum of four traffic shaping classes can be configured. Select the traffic shaping class number between 1 -4 to view details. If no class ID is specified, the system displays all configured traffic classes. • priority-map – Displays.1p to transmit priority map. • statistics {class <1-4>} – Displays traffic shaping class statistics. Select the traffic shaping class number between 1 -4 to view statistics.
upgrade-status {detail}	Displays the last image upgrade status. The 'detail' parameter displays detailed image upgrade information.
users	Displays active user (currently logged in users) information
version {verbose}	Displays software and hardware version details. The 'verbose' parameter displays detailed hardware and software version information.
virtual-ip [config|status]	Displays IP redundancy feature details • config – Displays virtual IP configuration • status – Displays virtual IP current status

wireless
[aap-version|ap|
ap-containment|
ap-detection-config|
ap-images|
ap-radio-config|
ap-unadopted|
authorized-aps|
channel-power|
client|config|
country-code-list|
default-ap|fw|
fwupdate-filelocation|
fwupdate-filename|
fwupdate-mode|
fwupdate-serveraddress|
fwupdate-username|
hotspot|
hotspot-config|
ignored-aps|known|
mac-auth-local|
mesh|
mobile-unit|
multicast-packet-limit|
non-preferred-ap-attempts-threshold|qos-mapping|
radio|radio-group|
regulatory|
self-healing-config|
sensor|smart-rf|
unauthorized-aps|
wips|
wireless-switch-statistics|
wlan]
	Displays wireless configuration commands
	• aap-version – Displays the minimum adaptive firmware version string
	• ap {<LIST>|config} – Displays adopted access port status
	  • <LIST> – Lists the MAC address of a single access port or a list of indices (for example, 1-4, 10) for detailed information
	  • config – Displays configured access port status
	• ap-containment [config|table] – Displays following rogue AP containment parameters:
	  • config – Displays rogue AP containment configuration
	  • table – Displays the rogue AP containment table
	• ap-detection-config – Displays detected AP configuration
	• ap-images – Lists access port images on the wireless switch
	• ap-radio-config [<MAC-ADDRESS>] – Displays AP radio configuration
	  • <MAC-ADDRESS> – The MAC address of the AP radio in the <AA-BB-CC-DD-EE-FF> format
	• ap-unadopted – Lists unadopted access ports
	• authorized-aps – Lists authorized APs detected by access port scans
	• channel-power [11a|11b|11bg] – Lists the available channel and power levels for the following radio types
	  • 11a – Radio type is 802.11a
	  • 11b – Radio type is 802.11b
	  • 11bg – Radio type is 802.11bg
	The following parameters are common to all three radio types:
	  • indoor – Radio is placed indoor
	  • outdoor – Radio is placed outdoor
	• client [exclude-list|include-list] – Displays wireless client configuration
	  • exclude-list – Displays exclude client list
	  • include-list – Displays include client list

	• config – Displays wireless LAN configuration
	• country-code-list – Lists the supported country names and the corresponding 2 letter ISO 3166 country codes
	• default-ap – Displays default access port information
	• fw [config] – Displays configurable firewall parameters
	• fwupdate-filelocation – Displays file location
	• fwupdate-filename – Displays file name
	• fwupdate-mode – Displays firmware upgrade mode
	• fwupdate-serveraddress – Displays SFTP server IP address
	• fwupdate-username – Displays login user name
	• hotspot [<query>] – Displays hotspot query string configuration
	• hotspot-config {<1-256>} – Displays the hotspot configuration for a WLAN of the index <1-256>
	• hotspot-config <1-256> – Displays the WLAN hotspot configuration for a WLAN with index between 1 - 256
	• ignored-aps – Displays ignored APs seen by access port scans
	• known {ap} – Displays known AP parameters.
	  • {ap <1-1024>} – Optional. Select the AP index between 1 - 1024.
	• mac-auth-local {<1-1000>} – Lists the mac-auth-local entries.
	  • <1-1000> – Optional. Select the mac-auth-local entry between 1 - 1000 to display.
	• mesh [statistics] – Displays mesh related statistics
	  • <1-32> – To view statistics for a specific mesh, select the mesh index between 1 - 32.

show [wireless] [mobile-unit]	• mobile-unit {<1-8192>|<AA-BB-CC-DD-EE-FF>|association-history| association-stats|probe-history|radio|roaming|statistics|voice|wlan} – Displays details of associated mobile units, based on the option selected • <1-8192> – Optional. Select the mobile unit index between 1 - 8192. • <AA-BB-CC-DD-EE-FF> – Optional. Specify the mobile unit MAC address. • association-history {<AA-BB-CC-DD-EE-FF>} – Optional. Displays mobile unit history. To view history of a specific mobile unit, specify its MAC address. • association-stats – Optional. Displays mobile unit statistics • probe-history [<1-200>|config-list] – Optional. Displays mobile unit probe history, based on the option selected • <1-200> – Select mobile unit index to view probe history • config-list – Lists probe history MAC addresses • radio [<1-4096>] – Optional. Displays mobile units associated with a specified radio. Specify the radio index between 1 - 4096. • roaming [database] – Optional. Displays mobile unit inter-switch roaming database • statistics {<1-8192>|<AA-BB-CC-DD-EE-FF>|summary|voice} – Optional. Displays mobile unit RF statistics. You can view RF statistics for a specified mobile unit by selecting one of the following options: • <1-8192> – Optional. The mobile unit index • <AA-BB-CC-DD-EE-FF> – Optional. The mobile unit MAC address • summary – Optional. Displays RF statistics summary of all currently associated mobile units • voice {<1-8192>|<AA-BB-CC-DD-EE-FF>} – Optional. Displays mobile unit voice statistics • voice – Optional. Displays voice call details • wlan [<1-256>] – Optional. Displays mobile units associated with a specified WLAN. Specify WLAN index between 1 -256.

show wireless	• multicast-packet-limit – Displays multicast packet limit
	• non-preferred-ap-attempts-threshold – Displays non preferred ap attempts threshold
	• qos-mapping {wired-to-wireless|wireless-to-wired} – Displays *Quality of Service* (QoS) mappings used for mapping wireless priorities and 802.1p / DHCP tags
	  • wired-to-wireless – Optional. Displays mappings used when traffic is switched from wired to wireless
	  • wireless-to-wired – Optional. Displays mappings used when traffic is switched from wireless to wired
	• radio {<1-4096>|admission-control|all|beacon-table|config|monitor-table|statistics|unadopted|uptime|voice} – Displays following radio related commands
	  • <1-4096> – Optional. Displays a specified radio configuration details. Select the radio index between 1 - 4096 to view configuration.
	  • admission-control [voice] – Optional. Displays admission control voice access statistics for all configured radios
	  • voice <1-4096> – To view admission control voice access statistics for a specified radio, select the radio index between 1 - 4096.
	  • all – Optional. Displays adopted and non-adopted radio status
	  • beacon-table – Optional. Displays radio-to-radio beacon table
	  • config {<1-4096>|default-11a|default-11an|default11bg|default-11bgn|} – Optional. Displays radio configuration, based on the option selected
	  • monitor-table – Optional. Displays radio-to-radio monitoring table
	  • statistics {<1-4096>|long-interval|short-interval|voice} –Optional. Displays radio statistics based on the option selected
	  • unadopted – Lists unadopted radios
	  • uptime – Displays uptime of all radios
	  • voice – Displays voice call details for all radios.
	  • <1-4096> – To view voice call details for a specific radio, select the radio index between 1 - 4096.
	• radio-group – Displays radio group configuration
	  • <1-256> – To view configuration of a specific radio group, specify the group index between 1 -256.
	• regulatory [<WORD>] – Displays wireless regulatory (allowed channel/ power) information for a specified country
	  • <WORD> – Specify the 2 letter ISO 3166 country code. Use the 'show > wireless > country-code-list' command to view supported country codes.

show wireless	• self-healing-config {<1-4096>|all} – Displays following self-healing parameters:
	  • <1-4096> – Displays self healing configuration for a specified radio. Select the radio index between 1 4096.
	  • all – Displays self healing configuration for all configured radios
	• sensor {<1-48>|default-config} – Displays *Wireless Intrusion Protection System* (WIPS) configuration.
	  • <1-48> – Displays WIPS configuration for a specified sensor. Select the sensor index between 1 - 48.
	  • default-config – Displays default WIPS configuration sensor settings.
	• smart-rf – Displays Smart-RF configuration, based on the option selected
	  • calibration-status – Displays Smart-RF calibration status
	  • configuration – Displays Smart-RF configuration
	  • history – Displays Smart-RF assignment history since latest calibration
	  • radio [config|local-status|map|master-status|neighbors|spectrum] – Displays radio related commands
	• unauthorized-aps – Displays unauthorized APs seen by access port or mobile unit scans
	• wips {configured-ap-def-essids|configured-bad-essids|fake-ap-flood|filter-list|suspicious-ap} – Displays WIPS parameters
	  • configured-ap-def-essids – Lists configured default ESSIDs
	  • configured-bad-essids – Lists configured bad ESSIDs
	  • fake-ap-flood [threshold] – Displays fake AP flood threshold
	  • filter-list – Lists currently filtered mobile units
	  • suspicious-ap [signal-strength-threshold] – Displays suspicious AP signal strength threshold
	• wireless-switch-statistics {detail} – Displays detailed wireless switch statistics
	• wlan [config|statistics] – Displays WLAN parameters
	  • config {<1-256>|all|enabled} – Displays WLAN configuration
	  • <1-256> – Displays configuration of a specified WLAN. Select the WLAN index between 1 - 256.
	  • all – Displays configuration of all configured WLANs
	  • enabled – Displays configuration of WLANs that are currently enabled
	  • statistics {<1-256>} – Displays WLAN statistics
	  • <1-256> – To view statistics of a specified WLAN, select the WLAN index between 1 - 256.

wlan-acl [<1-256>|all]	Displays WLAN based ACLs • <1-256> – Displays ACLs attached to the specified WLAN ID • all – Displays ACLs attached to WLAN port

Usage Guidelines

Refer to *show on page 2-25* for additional information.

Example

```
RFS7000#show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
```

```
  wlan-acl              wlan based acl
RFS7000#
```

4.1.22 terminal

Priv Exec Commands

Use this command to configure terminal display settings.

Syntax

```
terminal [length <0-512>|no|width <0-512>]
terminal no [length <0-512>|width]
```

Parameters

length <0-512>	Sets the number of lines displayed on the terminal screen between 0 - 512 (0 is for no pausing)
no [length <0-512>|width]	Negates or reverts the terminal Screen length and width settings • length <0-512> – Resets the number of lines displayed on the terminal screen • width – Resets the width of the terminal screen
width <0-512>	Sets the maximum number of characters displayed on the terminal screen per line between 0 - 512

Example

```
RFS7000#terminal length 200
RFS7000#

RFS7000#terminal width 300
RFS7000#

RFS7000#show terminal
Terminal Type: xterm
Length: 200     Width: 300
RFS7000#

RFS7000#terminal no length 200
RFS7000#

RFS7000#terminal no width
RFS7000#

RFS7000#show terminal
Terminal Type: xterm
Length: 24     Width: 80
RFS7000#
```

4.1.23 traceroute

Priv Exec Commands

Use this command to trace the route to a destination.

Syntax

```
traceroute [<WORD>|ip <WORD>]
```

Parameters

<WORD>	Traces the route to a specified destination address or hostname
ip <WORD>	IP trace. Traces the route to a specified destination address or hostname

Example

```
RFS7000#traceroute ip 172.16.10.10
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 38 byte packets
 1  172.16.10.10 (172.16.10.10)  0.825 ms  0.312 ms  0.366 ms
RFS7000#
```

4.1.24 upgrade

Priv Exec Commands

Use this command to upgrade the switch software image.

Syntax

```
upgrade URL {background}
```

Parameters

URL {background}	Defines location of firmware image • background – Optional. Performs firmware upgrade in the background

Example

```
RFS7000#upgrade ?
  URL  Location of firmware image
       URLs:  sftp://<user>@<hostname|IP>[:port]/path/file

RFS7000#upgrade
```

4.1.25 upgrade-abort

Priv Exec Commands

Use this command to abort an ongoing upgrade process.

Syntax

```
upgrade-abort
```

Parameters

None

Example

```
RFS7000#upgrade-abort
% Error: No upgrade in progress

RFS7000#upgrade tftp://xxx.xxx.xxx.xxx:/img

background
RFS7000#Sep 08 16:01:38 2011: %KERN-4-WARNING:

EXT3-fs warning: maximal mount
count reached, running e2fsck is recommended.
Sep 08 16:01:38 2011: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
%KERN-6-INFO: kjournald starting.  Commit

interval 5 seconds.
Sep 08 16:01:43 2011: %KERN-6-INFO: EXT3 FS on

hda6, internal journal.
Sep 08 16:01:43 2011: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered
data mode..
RFS7000#upgrade-abort
RFS7000#
RFS7000#show upgrade-status
Last Image Upgrade Status : Extracting files

(this can take some time).Aborted
Last Image Upgrade Time   : Fri Sep  8 16:01:54 2011
```

4.1.26 write

Priv Exec Commands

Use this command to write the running configuration to memory or terminal.

Syntax

```
write [memory|terminal]
```

Parameters

memory	Writes to *non-volatile* (NV) memory
terminal	Writes to the terminal

Example

```
RFS7000#write terminal
!
! configuration of RFS7000 version 1.0.0.0-016GR
!
version 1.1
!
!

username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
country-code us
logging buffered 4
logging console 4
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
no service pm sys-restart
service radius
license AP
8088bb045018988b3aa21321d4af9618bc68029885fbcc680a96194dfbeedc28400621446ca3a316
!
wireless
 wlan 1 enable
 wlan 1 ssid AJIT
radio add 1 00-15-70-14-FE-C4 11bg ap300
 radio 1 max-mobile-units 256
 radio add 2 00-15-70-14-FE-C4 11a ap300
 radio 2 max-mobile-units 256
 radio default-11a max-mobile-units 256
 radio default-11bg max-mobile-units 256
 radio default-11b max-mobile-units 256
 no ap-ip default-ap switch-ip
!.....................................
```

5

Global Configuration Commands

The term **global** is used to indicate characteristics or features effecting the system as a whole. Use the Global configuration mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the *configure terminal* command, under PRIV EXEC, to enter the global configuration mode.

The example below describes how to enter the global configuration mode from the privileged EXEC mode:

```
RFS7000# configure terminal
RFS7000(config)#
```

NOTE The system prompt changes to indicate you are in global configuration mode. The prompt for global configuration mode consists of the host-name of the device followed by (config) and the pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *copy running-config startup-config* EXEC mode command is issued.

5.1 Global Configuration Commands

Table 5.1 summarizes the Global Config commands.

Table 5.1 Global Configuration Command Summary

Command	Description	Ref.
aaa	Configures the *Authentication, Authorization, and Accounting* (AAA) parameters	*page 5-4*
aap-wlan-acl	Applies an ACL on WLAN for AAP	*page 5-5*
access-banner	Customizes the switch's access banner	*page 5-6*
access-list	Adds an access list entry	*page 5-7*
arp	Configures *Address Resolution Protocol* (ARP) parameters	*page 5-14*
audit-log-filter	Adds or deletes audit event log filters	*page 5-15*
auth-timeout	Sets authentication timeout value	*page 5-17*
autoinstall	Displays autoinstall configuration commands	*page 5-18*
boot	Reboots the switch	*page 5-19*

Command	Description	Ref.
bridge	Configures bridge parameters	*page 5-20*
clrscr	Clears the display screen	*page 2-2*
country-code	Configures the country of operation. This erases all existing radio configuration	*page 5-22*
crypto	Configures data encryption parameters	*page 5-23*
do	Runs commands from the EXEC mode	*page 5-28*
end	Ends the current mode and moves to the EXEC mode	*page 5-29*
errdisable	Enables the port timeout mechanism	*page 5-30*
exit	Ends the current mode and moves to the previous mode	*page 2-3*
firewall	Configures wireless firewall parameters	*page 5-31*
help	Describes the interactive help system	*page 2-4*
hostname	Sets the system's network name	*page 5-33*
interface	Configures an interface	*page 5-34*
ip	Configures *Internet Protocol* (IP) components	*page 5-35*
license	Adds a license to a feature	*page 5-44*
line	Configures a terminal line	*page 5-45*
local	Configures the local user's name and password for VPN authentication	*page 5-46*
logging	Modifies message logging facilities	*page 5-47*
mac	Configures MAC ACLs	*page 5-49*
mac-address-table	Configures MAC address table	*page 5-50*
mac-name	Maps a MAC name to a MAC address	*page 5-51*
management	Sets the management interface properties	*page 5-52*
network-element-id	Sets the system's network element ID	*page 5-53*
no	Negates a command or set its defaults	*page 2-6*
ntp	Configures *Network Time Protocol* (NTP) parameters	*page 5-54*
prompt	Sets the system prompt	*page 5-58*
radius-server	Enters radius-server mode	*page 5-59*
ratelimit	Enables ratelimit logging parameters	*page 5-60*
redundancy	Configures redundancy group parameters	*page 5-61*

Command	Description	Ref.
remote-login	Configures remote login parameters	*page 5-64*
role	Configures role parameters	*page 5-65*
rtls	Configures *Real Time Location System* (RTLS) mode parameters	*page 5-66*
service	Service commands	*page 5-67*
show	Shows running system information. For more information see, *show on page 2-25*.	*page 5-70*
smtp-notification	Modifies *Simple Mail Transfer Protocol* (SMTP) notification parameters	*page 5-83*
snmp-server	Modifies *Simple Network Management Protocol* (SNMP) engine parameters	*page 5-85*
spanning-tree	Spanning tree commands	*page 5-87*
timezone	Configures the timezone	*page 5-91*
traffic-shape	Configures traffic/packet shaping parameters	*page 5-90*
username	Establishes user name authentication	*page 5-91*
virtual-ip	Configures the virtual IP parameters of the switch	*page 5-92*
vpn	Configures VPN commands	*page 5-94*
wireless	Configures wireless parameters	*page 5-95*
wlan-acl	Applies an ACL on the WLAN port	*page 5-96*
zeroize	Enables zeroization of critical security parameters	*page 5-98*

5.1.1 aaa

Global Configuration Commands

Use this command to configure current *Authentication, Authorization and Accounting* (AAA) login settings.

Syntax

```
aaa [authentication|nas|vpn-authentication]

aaa authentication login default [local {radius}|radius {local}]
aaa nas <NAME>
aaa vpn-authentication [primary|secondary] [<IP-Address>] [key] [0 <WORD>|
  2 <WORD>|<WORD>]
```

Parameters

authentication [login]	Configures authentication parameters
	• login – Configures the default login authentication list
	  • default – Configures one of the following default authentication list:
	  • local {radius} – Local user database
	  • radius {local} – External RADIUS server

nas <WORD>	Configures the *Network Access Server* (NAS) originating the *Remote, Authentication Dial-in User Service* (RADIUS) access request (for VPN only) • <WORD> – Specify the NAS server name (a string not exceeding 64 characters in length).

vpn-authentication [primary|secondary] <IP-Address> [key] [0 <WORD>| 2 <WORD>| <WORD>]	Configures the RADIUS server settings
	• [primary|secondary] – Configures the primary/secondary RADIUS server parameters
	The following parameters are common to the 'primary' and 'secondary' keywords:
	• <IP-Address> – The RADIUS server's IP address
	  • key – The RADIUS client preshared key. This must match with the RADIUS server.
	  • 0 <WORD> – Password is specified UNENCRYPTED
	  • 2 <WORD> – Password is encrypted with password encryption secret
	  • <WORD> – Specify the shared secret (should not exceed 32 characters in length)

Usage Guidelines

Use AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

Example

```
RFS7000(config)#username motorolaadmin password motorola

RFS7000(config)#username motorolaadmin privilege  superuser

RFS7000(config)#aaa authentication login default local
RFS7000(config)#
```

5.1.2 aap-wlan-acl

Global Configuration Commands

Use this command to apply an *Access Control List* (ACL) on WLAN for AAP.

Syntax

```
aap-wlan-acl <1-256> [<100-199>|<WORD>] [in|out]
```

Parameters

aap-wlan-acl	Applies an IP extended ACL on an independent WLAN for an AAP
<1-256> [<100-199>|<WORD>]	Select an independent WLAN index between 1 - 256. • <100-199> – Select the IP extended ACL index between 100 - 199. • <WORD> – Specify the ACL name (with permit or deny rules).
in	This parameter is common to the '<100-199>' and '<WORD>' keywords. • Displays incoming packets
out	This parameter is common to the '<100-199>' and '<WORD>' keywords. • Displays Outgoing packets

Usage Guidelines

AAP IP filtering cannot be applied for extended WLANs.

Example

```
RFS6000(config)#aap-wlan-acl 6 symbol in
RFS6000(config)#

RFS6000(config)#aap-wlan-acl 6 125 out
RFS6000(config)#
```

5.1.3 access-banner

Global Configuration Commands

Use this command to customize the switch's access banner.

Syntax

```
access-banner [<LINE>]
```

Parameters

<LINE>	Enter a string with minimum 10 characters and maximum 250 characters.

Example

```
RFS7000(config)#access-banner "Welcome to my switch CLI"
RFS7000(config)#

RFS7000(config)#show access-banner
Welcome to my switch CLI
RFS7000(config)#
```

5.1.4 access-list

Global Configuration Commands

Use this command to add an *Access Control List* (ACL) entry. Use the access list command under global configuration to configure the access list mechanism for filtering frames by protocol type or vendor code.

ACLs control access to the network through a set of rules. Each rule specifies an action taken when a packet matches it, within the given set of rules. If the action is deny, the packet is dropped and if the action is permit, the packet is allowed. The following ACLs are supported by the switch:

- IP Standard ACl
- IP Extended ACL
- MAC Extended ACL

ACLs are identified by a number or a name. Numbers are predefined for IP Standard and Extended ACLs, and the name can be any valid alphanumeric string (not extending 64 characters). With numbered ACLs, the rule parameters have to be specified on the same command line along with the ACL identifier.

Syntax

For Standard IP ACLs:

```
access-list [<1-99>|<1300-1999>] [deny|permit|mark]
access-list [<1-99>|<1300-1999>] [deny|permit] [<A.B.C.D/M>|any|host <A.B.C.D>]
  {log (rule-precedence <1-5000>)}
access-list [<1-99>|<1300-1999>] mark [8021p <0-7>|dscp <0-63>|tos <0-255>]
  [<A.B.C.D/M>|any|host <A.B.C.D>] {log (rule-precedence <1-5000>)}
For Extended IP ACLs:
access-list [<100-199>|<2000-2699>] [deny|permit|mark [8021p <0-7>|dscp <0-63>|
  tos <0-255>]] [icmp|ip|proto|tcp|udp]

access-list [<100-199>|<2000-2699>] [deny|permit|mark [8021p <0-7>|dscp <0-63>|
  tos <0-255>]] [ip] [source/source-mask|host-source|any]
  [destination/destination-mask|host-destination|any] {<icmp-type>} {<icmp-code>}
  (log {rule-precedence <WORD>|rule-precedence <1-5000>})

access-list [<100-199>|<2000-2699>] [deny|permit|mark [8021p <0-7>|dscp <0-63>|
  tos <0-255>]] [icmp] [source/source-mask|host-source|any]
  [destination/destination-mask|host-destination|any] {<icmp-type>} {<icmp-code>}
  (log {rule-precedence <WORD>|rule-precedence <1-5000>})

access-list [<100-199>|<2000-2699>] [deny|permit|mark [8021p <0-7>|dscp <0-63>|
  tos <0-255>]] [tcp|udp] [source/source-mask|host-source|any]
  [destination/destination-mask|host-destination|any|eq <1-65535>|range <1-65535>]
  {(eq <OPTION>|log|range <1-65535>|rule-precedence <WORD>|rule-precedence <1-5000>)}

access-list [<100-199>|<2000-2699>] [deny|permit|mark [8021p <0-7>|dscp <0-63>|
  tos <0-255>]] [proto] [<1-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp]
  [source/source-mask|host-source|any] [destination/destination-mask|host-destination|
  any] (log {rule-precedence <WORD>|rule-precedence <1-5000>})
```

NOTE To create a named ACL, use `ip access-lsit` (Standard/Extended). For more details check *ip on page 5-35*.

Using `access-list [<100-199>|<2000-2699>]` moves to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Config Commands on page 14-1*.

Using `access-list [<1-99>|<1300-1999>]` moves to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Config Commands on page 15-1*.

Parameters

access-list
[<1-99>|<1300-1999>]
[deny|permit|
mark [8021p <0-7>|
dscp <0-63>|
tos <0-255>]]
[<A.B.C.D/M>|
host <A.B.C.D>|any]
{log
(rule-precedence <1-5000>)}
	Adds a **Standard IP** access control list entry
	• [<1-99>|<1300-1999>] – Defines the access list number between 1 - 99 or 1300 - 1999
	• [deny|permit|mark] – Defines following ACL action types:
	  • deny – Specifies packets to reject
	  • permit – Specifies packets to forward.mark [8021p|dscp|tos] – Specifies packets to mark. The action type `mark` is functional only over a port ACL.
	  • 8021p <0-7> – Specifies 8021p priority values between 0 - 7
	  • dscp <0-63> – Modifies the *Differentiated Service Code Point* (DSCP) bits in the IP header between 0 - 63
	  • tos <0-255> – Specifies *Type of Service* (TOS) value between 0 - 255. (least significant 2 bits must be 0)
	The following are common to the 'deny', 'permit', and 'mark [802|dscp|tos]' keywords:
	• [<A.B.C.D/M>|host <A.B.C.D >|any] – 'Source' defines the source address of the network or host in dotted decimal format. 'Source-mask' is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP used for matching.
	• any – The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0.
	• host <A.B.C.D > – The keyword **host** is an abbreviation for exact source (<A.B.C.D>) and source-mask bits equal to 32.
	  • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	  • (rule-precedence <1-5000>) – Optional. Specifies the integer value between
	1- 5000 (this value sets the rule precedence in the ACL)

access-list [<100-199>|<2000-2699>] [deny|permit| mark [8021p <0-7>| dscp <0-63>| tos <0-255>]] [**ip**] [source/source-mask| host-source|any] [destination/destination-mask| host-destination|any] {log (rule-description| rule-precedence)}	Adds an **Extended IP** access list entry using the **ip** keyword
	• [<100-199>|<2000-2699>] – For IP type of extended ACL, the ACL number must be between 100 - 199
	• [deny|permit|mark] – Defines following ACL action types:
	  • deny – Specifies packets to reject
	  • permit – Specifies packets to forward
	  • mark [8021p|dscp|tos] – Specifies packets to mark. The action type `mark` is functional only over a Port ACL.
	  • 8021p <0-7> – Specifies 8021p priority values between 0 - 7
	  • dscp <0-63> – Modifies the DSCP bits in the IP header between 0 - 63
	  • tos <0-255> – Specifies TOS value between 0 - 255. (least significant 2 bits must be 0)
	The following are common to the 'deny', 'permit', and 'mark [8021p|dscp|tos]' keywords:
	• [**ip**] [source/source-mask|host-source|any] – Specifies IP as the protocol
	  • [source/source-mask] – 'Source' defines the source address of the network or host in dotted decimal format. 'Source-mask' is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP used for matching.
	  • host-source – The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
	  • any – The keyword **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
	  • [destination/destination-mask|host-destination|any] – Defines the destination host IP address or destination network address
	  • host-destination – Defines the exact destination host IP address
	  • any – Defines any destination host IP
	After specifying the source and destination network/host, specify the following:
	• log {rule-description|rule-precedence} – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	• rule-description <WORD> – Optional. The ACL entry description (not exceeding 128 characters)
	• [rule-precedence <1-5000> – Optional. The ACL entry precedence value between 1- 5000 (this value sets the rule precedence in the ACL)

access-list [<100-199>|<2000-2699>] [deny|permit| mark [8021p <0-7>| dscp <0-63>|tos <0-255>]] [**icmp]** [source/source-mask| host- source|any] [destination/destination-mask|host-destination| any] [<icmp-type>] [<icmp-code>] {log {rule-precedence| rule-precedence}}	Adds an **Extended IP** access list entry using the **icmp** keyword
	• [<100-199>|<2000-2699>] – For ICMP extended ACLs, the ACL number must be between 2000-2699
	• [deny|permit|mark] – Defines following ACLaction types:
	  • deny – Specifies packets to reject
	  • permit – Specifies packets to forward
	  • mark [8021p|dscp|tos] – Specifies packets to mark. The action type `mark` is functional only over a port ACL.
	  • 8021p <0-7> – Specifies 8021p priority values between 0 - 7
	  • dscp <0-63> – Modifies the DSCP TOS bits in the IP header, for the DSCP code point value, between 0 - 63
	  • tos <0-255> – Specifies TOS value between 0 - 255. (least significant 2 bits must be 0)
	The following are common to the 'deny', 'permit', and 'mark [8021p|dscp|tos]' keywords:
	• [**icmp**] [source/source-mask|host-source|any] – Specifies ICMP as the protocol
	  • [source/source-mask] – 'Source' defines the source address of the network or host in dotted decimal format. 'Source-mask' is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP used for matching.
	  • host-source – The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
	  • any – The keyword **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
	  • [destination/destination-mask|host-destination|any] – Defines the destination host IP address or destination network address
	  • host-destination – Defines the exact destination host IP address
	  • any – Defines any destination host IP
	After specifying the source and destination network/host, specify the following:
	• [icmp-type |icmp-type icmp-code] – Optional. The **ICMP type** value from 0 - 255. The **ICMP code** value from 0 - 255 (valid only for ICMP)
	• log {rule-description|rule-precedence} – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	• rule-description <WORD> – Optional. The ACL entry description (not exceeding 128 characters)
	• [rule-precedence <1-5000> – Optional. The ACL entry precedence value between 1- 5000 (this value sets the rule precedence in the ACL)

access-list [<100-199>|<2000-2699>] [deny|permit| mark [8021p <0-7>| dscp <0-63>|tos <0-255>]] [**tcp|udp]** [source/source-mask| host-source|any] [destination/destination-mask|host-destination| any|eq <1-65535>| range <1-65535>] {(eq <OPTION>|log| range <1-65535>| rule-description <WORD>|rule-precedence <1-5000>)}	Adds an **Extended IP** access list entry using the **tcp** or **udp** keywords
	• (<100-199>|<2000-2699>) – For TCP or UDP type of extended ACL, the ACL number must be between 2000 - 2699
	• [deny|permit|mark] – Defines following ACl action types:
	  • deny – Specifies packets to reject
	  • permit – Specifies packets to forward
	  • mark [8021p|dscp|tos] – Specifies packets to mark. The action type `mark` is functional only over a Port ACL.
	  • 8021p <0-7> – Specifies 8021p priority values between 0 - 7
	  • dscp <0-63> – Modifies the DSCP TOS bits in the IP header, for the DSCP code point value, between 0 - 63
	  • tos <0-255> – Specifies TOS value between 0 - 255. (least significant 2 bits must be 0)
	The following are common to the 'deny', 'permit', and 'mark [8021p|dscp|tos]' keywords:
	• [**tcp**|**udp**] [source/source-mask|host-source|any] – Specifies TCP or UDP as the protocol
	  • [source/source-mask] – 'Source' is the source address of the network or host in dotted decimal. 'Source-mask' is the network mask. For example,10.1.1.10/24 indicates that the first 24 bits of the source IP are used for matching.
	  • any – An abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0
	  • host – An abbreviation for an exact source (A.B.C.D) and source-mask bits equal to 32
	  • [destination/destination-mask|host destination|any] – Optional. The destination host IP address or destination network address
	  • [log] – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	  • [rule-precedence access-list-entry precedence] – Optional. Integer value between 1- 5000 (this value sets the rule precedence in the ACL)

access-list
[<100-199>|<2000-2699>]
[deny|permit|
mark [8021p <0-7>|
dscp <0-63>|
tos <0-255>]]
[**proto**]
[<1-254>|
<WORD>|eigrp|gre|
igmp|igp|ospf|vrrp]
[source/source-mask|
host-source|any]
[destination/destination-mask|
host-destination|any]
{log (rule-description|
rule-precedence)}
	Adds an **Extended IP** access list entry using the **proto** keyword
	The following are common to the 'deny', 'permit', and 'mark [8021p|dscp|tos]' keywords:
	• [**proto**] [<1-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] –
	  • <1-254> – Specifies any protocol number
	  • <WORD> – Specifies any protocol name
	  • eigrp – Specifies the *Enhanced Interior Gateway Routing Protocol* (EIGRP) protocol 88
	  • gre – Specifies the *Generic Routing Encapsulation* (GRE) protocol 47
	  • igmp – Specifies the *Internet Group Management Protocol* (IGMP) protocol 2
	  • igp – Specifies the *Interior Gateway Protocol* (IGP) protocol 9
	  • ospf – Specifies the *Open Shortest Path First* (OSPF) protocol 89
	  • vrrp – Specifies the *Virtual Routing Redundancy Protocol* (VRRP) protocol 112
	After specifying the protocol type, specify the source and destination network/host IP addresses.
	• [source/source-mask|host-source|any] – Specifies IP as the protocol
	  • [source/source-mask] – 'source' defines the source address of the network or host in dotted decimal format. 'source-mask' is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP used for matching.
	  • host-source – The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
	  • any – The keyword **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
	  • [destination/destination-mask|host-destination|any] – Defines the destination host IP address or destination network address
	  • host-destination – Defines the exact destination host IP address
	  • any – Defines any destination host IP
	After specifying the source and destination network/host, specify the following:
	• log {rule-description|rule-precedence}– Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	• rule-description <WORD> – Optional. The ACL entry description that does not exceed 128 characters
	• [rule-precedence <1-5000> – Optional. The ACL entry precedence value between
	1- 5000 (this value sets the rule precedence in the ACL)

Usage Guidelines

Use an access list command under global configuration to create an access list. The switch supports port, router and WLAN ACLs.

- When the access list is applied on an Ethernet port, it becomes a port ACL.
- When the access list is applied on a VLAN interface, it becomes a router ACL.
- When the access list is applied on a WLAN index, it becomes a WLAN ACL.

A MAC access list, to allow an ARP, is mandatory for both port and WLAN ACLs. For more information on how to configure a MAC access list, see *permit on page 16-12*.

Example

The example below creates a standard *access list* (ACL) to permit traffic coming to the interface.

```
RFS7000(config)#access-list 1 permit any
RFS7000(config)#
```

The example below creates a extended IP access list to permit IP traffic between two networks.

```
RFS7000(config)#access-list 101 permit ip 192.168.1.0/24 192.168.2.0/24
RFS7000(config)#
```

The example below creates an extended access list to permit TCP traffic, between two networks, with a destination port range between 20 and 23.

```
RFS7000(config)#access-list 101 permit tcp 192.168.1.0/24 192.168.2.0/24 range 20 23
RFS7000(config)#
```

The example below denies ICMP traffic from any source to any destination.

```
RFS7000(config)#access-list 115 deny icmp any any
RFS7000(config)#access-list 115 permit ip any any
RFS7000(config)#
```

5.1.5 arp

Global Configuration Commands

Use this command to map an IP address to a MAC address recognized on the managed network. The *Address Resolution Protocol* (ARP) enables mapping of IP to MAC addresses. This conversion is possible in both directions.

Syntax

```
arp [<IFNAME>|ge <1-4>|me1|sa <1-4>|vlan <1-4094>] [<IP-ADDRESS>] [MAC-ADDRESS]
```

Parameters

<IFNAME>	The interface name
ge <1-4>	The GigabitEthernet interface. There are a maximum of four GigabitEthernet interfaces. Select the interface index between 1 - 4.
me1	The FastEthernet interface
sa <1-4>	The StaticAggregate interface. There are a maximum of four StaticAggregate interfaces. Select the interface index between 1 - 4.
vlan <1-4094>	The VLAN switch interface. Select the VLAN interface index between 1 - 4094.
<IP-ADDRESS>	This parameter is common to all of the above interface types. Specify the IP address to be mapped with a specified MAC address.
<MAC-ADDRESS>	This parameter is common to all of the above interface types. Specify the MAC address to be mapped with a IP address specified by the <IP-ADDRESS> parameter.

Example

```
RFS7000(config)#arp TestIF ?
  A.B.C.D  Internet Protocol (IP)

RFS7000(config)#arp TestIF 1.2.3.4 ?
  AA-BB-CC-DD-EE-FF  MAC Address

RFS7000(config)#arp TestIF 1.2.3.4 11-22-33-44-55 ?
  <cr>
```

5.1.6 audit-log-filter

Global Configuration Commands

Use this command to add or delete audit event log filters.

NOTE When no filters are set the default action is to *permit any.*

Syntax

```
audit-log-filter [add|delete]

audit-log-filter add <1-10> [deny|permit] [<USERNAME>|any] [any|console|network]

audit-log-filter add <1-10> [deny|permit] [<USERNAME>|any] [any|network] [<MAC>|any]
  [<IP>|any]
```

Parameters `audit-log-filter delete <1-10>`

add <1-10> [deny|permit]	Adds this rule to the filtering logic • <1-10> – Specifies the rule precedence index • deny – Disables logging • permit – Enables logging • <USERNAME> – The user defined username (username should be of length between 1 - 28) or any username • any – Any username. The following are common to the 'deny' and 'permit' parameters: • any – Enables any login source • console – Enables console login only • network – Enables network logging only The following are common to the 'any' and 'network' parameters: • [<MAC>|any] – Specifies a MU's MAC address or any MU MAC address in the AA-BB-CC-DD-EE-FF format • [<IP>|any] – Specifies the client's IP address or any IP address in the A.B.C.D format
delete	Deletes a specified rule from the filtering logic • <1-10> – Specify the rule precedence index between 1 - 10.

Example

```
RFS7000(config)#audit-log-filter add 1 permit any any any any
RFS7000(config)#

RFS7000(config)#show audit-log-filters
  RULE-PRECEDENCE  USER NAME SOURCE     MAC-address  IP-address    ACTION
  1                any         any      any           any           permit
RFS7000(config)#

RFS7000(config)#audit-log-filter delete 1
RFS7000(config)#


RFS7000(config)#show audit-log-filters
  RULE-PRECEDENCE  USERNAME SOURCE    MAC-address        IP-address          ACTION
RFS7000(config)#
```

5.1.7 auth-timeout

Global Configuration Commands

Use this command to set the authentication timeout in minutes.

Syntax

```
auth-timeout <1-1440>
```

Parameters

<1-1440>	Specify the authentication timeout between 1 - 1440 minutes.

Example

```
RFS7000(config)#auth-timeout 10 ?
  <cr>

RFS7000(config)#
```

5.1.8 autoinstall

Global Configuration Commands

Use this command to configure autoinstall parameters.

Syntax

```
autoinstall [clear-config-history|cluster-config {<URL>}|config {<URL>}|
  image {<URL>|version <WORD>}|reset-config|start]
```

Parameters

autoinstall	Displays autoinstall configuration commands
clear-config-history {<URL>}	Autoinstalls clear configuration history setup (this allows or causes reversion of image upgrades etc.)
cluster-config {<URL>}	Autoinstalls cluster configuration setup • <URL> – Optional. Provide the remote/external file location in the following formats: URLs: tftp://<hostname|IP>/path/file ftp://<user>:<passwd>@<hostname|IP>/path/file [tftp port (69) / ftp port (21) are fixed]
config {<URL>}	Autoinstalls configuration setup • <URL> – Optional. Provide the remote/external file location in the following formats: URLs: tftp://<hostname|IP>/path/file ftp://<user>:<passwd>@<hostname|IP>/path/file [tftp port (69) / ftp port (21) are fixed]
image {<URL>|version}	Autoinstalls expected image version changes • <URL> – Optional. Provide the remote/external image location in the following formats: URLs: tftp://<hostname|IP>/path/file ftp://<user>:<passwd>@<hostname|IP>/path/file [tftp port (69) / ftp port (21) are fixed] • version <WORD> – Optional. Provide the image version string.
reset-config	Resets all autoinstall features to factory defaults
start	Starts the autoinstall sequence

Example

```
RFS7000(config)#autoinstall clear-config-history
RFS7000(config)#
```

5.1.9 boot

Global Configuration Commands

This command reboots the switch with an image present in the mentioned partition (either the primary or secondary partition).

Syntax

```
boot [system] [primary|secondary]
```

Parameters

system [primary|secondary]	Specifies the boot image used after reboot • primary – Specifies the primary image • secondary – Specifies the secondary image

Example

```
RFS7000(config)#boot system primary
Wireless switch will be rebooted, do you want to continue? (y/n):y
Do you want to save the configuration? (y/n):y

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
```

5.1.10 bridge

Global Configuration Commands

Use this command to configure bridge-specific details.

Syntax

```
bridge [<1-32>|multiple-spanning-tree]

bridge <1-32> [address|ageing-time]

bridge <1-32> [address] [MAC-ADDRESS] [discard|forward] [<IFNAME>|ge <1-4>|me1|
  sa <1-4>|vlan <1-4094>] [vlan <2-4094>]

bridge <1-32> [ageing-time] [0|<10-1000000>]

bridge multiple-spanning-tree [enable]
```

Parameters

<1-32> [address|ageing-time]	Specifies the bridge groups available for bridging. Select the bridge group index between 1 - 32. • address – Sets the address of the selected bridge group • ageing-time – Sets the time a learned MAC address persists after the last update

[address] [MAC-ADDRESS] [discard|forward] [<IFNAME>|ge <1-4>| sa <1-4>| vlan <1-4094>]	Sets the MAC address of the interface selected for bridging, in the `HHHH.HHHH.HHHH` format
	• discard – Discards the MAC address
	• forward – Forwards the MAC address
	  • <IFNAME> – The interface name
	  • me1 [vlan <2-4094>] – The FastEthernet interface
	  • ge <1-4> [vlan <2-4094>] – The GigabitEthernet interface index
	  • sa <1-4> [vlan <2-4094>] – The StaticAggregate interface index
	  • vlan <1-4094> [vlan <2-4094>] – The VLAN interface index
	  • vlan [2-4094] – Specify the VLAN ID between 2 - 4094

<1-32> [ageing-time] [0|<10-1000000>]	Sets the time a learned MAC address persists after the last update • [ageing-time] [0|<10-1000000>] – Sets the ageing time (in seconds) • 0 – Disables ageing<10-1000000> – Sets ageing time between 10 - 1000000 seconds
multiple-spanning-tree [enable]	Enables *Multiple Spanning Tree Protocol* (MSTP) commands

Usage Guidelines

Use `bridge multiple-spanning-tree` command to enable or disable MSTP globally. Use the `no` command with bridge-forward parameters to disable MSTP and change all ports to forwarding state.

Example

```
RFS7000(config)#bridge multiple-spanning-tree enable
RFS7000(config)

RFS7000(config)#show spanning-tree mst
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 800000157037fdf3
% 1: CIST Reg Root Id 800000157037fdf3
% 1: CST Bridge Id 800000157037fdf3
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability configured - Current cisco interoperability off
%
%   Instance        VLAN
RFS7000(config)#
```

5.1.11 country-code

Global Configuration Commands

Use this command to configure the country of operation.

Syntax

```
country-code
```

Parameters

None

Usage Guidelines

This command erases all existing radio configurations.

Example

```
RFS7000(config)#country-code ?
  WORD  the 2 letter ISO-3166 country code ("show wireless country-code-list" to see
list of supported countries)

RFS7000(config)#country-code us
RFS7000(config)#
```

5.1.12 crypto

Global Configuration Commands

Use this command to configure data encryption parameters.

NOTE `crypto isakmp(policy)Priority` leads you to config-crypto-isakmp instance. For more details see *Crypto ISAKMP Config Commands on page 6-1*.

`crypto isakmp(client)configuration group default` leads you to config-crypto-group instance. For more details see *Crypto Group Config Commands on page 7-1*.

`crypto isakmp(peer)IP Address` leads you to config-crypto-peer instance. For more details see *Crypto Peer Config Commands on page 8-1*.

`crypto ipsec transformset (name) <value>` leads you to config-crypto-ipsec. Use the crypto IPSEC transform-set command to define the transform configuration for securing data (e.g., esp-aes, esp-shahmac, etc.). The transform-set is then assigned to a crypto map using the map's set transform-set command. For more details see *Crypto IPSec Config Commands on page 9-1*.

`config-crypto-map` leads to config-crypto-map instance. For more information, see *Crypto Map Config Commands on page 10-1*.

`crypto pki trustpoint` mode leads to `(config-trustpoint)` instance. For more information, see *Trustpoint Config commands on page 11-1*.

Syntax

```
crypto [ipsec|isakmp|key|map|pki]

crypto ipsec [security-association|transform-set]
crypto ipsec security-association [lifetime] [kilobyte|seconds] <WORD>
crypto ipsec transform-set [SET-NAME] [esp-aes|esp-aes-192|esp-aes-256]
  {esp-sha-hmac}

crypto isakmp [client|keepalive|key|peer|policy]
crypto isakmp client [configuration] [group] [default]
crypto isakmp keepalive [<10-3600>]
crypto isakmp key [0 <WORD>|2 <WORD>|<WORD>] [address <IP-Address>|hostname <HOSTNAME>]
crypto isakmp peer [address <IP-Address>|dn <DISTINGUISHED-NAME>|hostname <HOSTNAME>]
crypto isakmp policy [<1-10000>]

crypto key [export|generate|import|zeroize]
crypto key export [rsa] [<RSAKeypair>] [URL] [<PASSPHRASE>]
crypto key generate [rsa] [<RSAKeypair>]
crypto key import [rsa] [<RSAKeypair>] [URL] [<PASSPHRASE>]
crypto key zeroize [rsa] [<RSAKeypair>]

crypto map [MAP-NAME] [<SEQUENCE-NUMBER>] [ipsec-isakmp|ipsec-manual] {dynamic}

crypto pki [authenticate|enroll|export|import|trustpoint]
crypto pki authenticate [<TRUSTPOINT-NAME>] [terminal|<URL>]
crypto pki enroll [<TRUSTPOINT-NAME>] [request|self-signed]
crypto pki export [<TRUSTPOINT-NAME>] [request|trustpoint] [<URL>]
crypto pki import [<TRUSTPOINT-NAME>] [certificate|crl|trustpoint] (terminal|<URL>)
crypto pki trustpoint [<TRUSTPOINT-NAME>]
```

Parameters

crypto (ipsec)	

ipsec [security-association| transform-set]	Configures *IP Security* (IPSec) policies
	• security-association – Sets the IPSec *security association* (SA) parameter
	  • lifetime [kilobyte|seconds] – Sets IPSec SA lifetime (can be defined in either in kilobytes or seconds).This is an IPsec Phase 2 SA lifetime.
	  • kilobytes – Volume-based key duration. Minimum is 500 KB and maximum is 204800 KB. The default value is 204800 KB.
	  • seconds – Time-based key duration (minimum is 90 seconds and maximum is 28800 seconds. The default value is 3600 seconds.
	Note: A security association expires after one of these two SA lifetimes is reached.
	• transform-set [<SET-NAME>] – Uses the crypto IPSec transform-set command to define the transform configuration for securing data
	  • esp-aes – *Encapsulating Security Payloads* (ESP) transform, using AES cipher
	  • esp-aes-192 – ESP transform, using AES cipher (192 bites)
	  • esp-aes-256 – ESP transform, using AES cipher (256 bites)
	  • esp-sha-hmac – Optional. Configures HMAC-SHA authentication for all of the above four ESP transforms
	The transform-set is then assigned to a crypto map using the map's set transform-set command. See *Crypto Map Config Commands on page 10-1*.

crypto (isakmp)	

isakmp [client|keepalive|key|peer|policy]	Configures *Internet Security Association and Key Management Protocol* (ISAKMP) policy
	• [client] [configuration] [group] [default] – This leads to the `config-crypto-group` instance. For more details, see*Crypto Group Config Commands on page 7-1*.
	• keepalive <10-3600> – Sets a keepalive interval for use with remote peers (defines the number of seconds between *Dead Peer Detection* (DPD) messages)
	• key [0 <WORD>|2 <WORD>|<WORD>] [address|hostname] – Sets a pre-shared key for remote peer
	  • 0 <WORD> – Password is specified UNENCRYPTED. Specify a key of minimum size 8 characters.
	  • 2 <WORD> – Password is encrypted with password-encryption secret. Specify a key of minimum size 8 characters.
	  • <WORD> – User provided password of minimum 8 characters
	  • address <A.B.C.D> – Defines the IP address of the peer with whom the key is shared. Specify the IP address in the A.B.C.D format.
	  • hostname – Defines the hostname of the peer with whom the key is shared
	• peer [address|dn|hostname] – Sets a remote peer. Use one of the following options to specify the remote peer:
	  • address <A.B.C.D> – The remote peer's IP address in the A.B.C.D format
	  • dn <DISTINGUISHED-NAME> – The remote peer's distinguished name
	  • hostname – The remote peer's hostname
	• policy <1-10000> – Sets policy for an ISAKMP protection suite. Select a sequence number for the ISAKMP protection suite between 1 - 10000.

key [export|generate|import|zeroize]	Enables authentication key management • [export] [rsa] [<RSAKeypair>] [URL <sftp>] [passphrase] – Exports keypair related configuration to a specified URL. Encrypts the keypair with the passphrase provided, before exporting • [generate] [rsa] [<RSAKeypair>] – Generates a RSA keypair (keypair size is 2048 bits) • [import] [rsa] [<RSAKeypair>] [URL <sftp>] [passphrase] – Imports keypair related configuration. Encrypts the keypair with the passphrase provided, before importing The following are common to all of the above keywords: • rsa <RSAKeypair> – The RSA keypair identifier associated with keypair • URL – The URL for exporting or importing the key. It can be provided in the following format: • sftp://<user>@<IP>/path/file • [zeroize] [rsa] [<RSAKeypair>] – Deletes a keypair. Specify the keypair name to delete.

map <CRYPTOMAP-NAME> <1-1000> [ipsec-isakmp| ipsec-manual] {dynamic}	Specifies a name for the new crypto map at the time of creation. For more details see *Crypto Map Config Commands on page 10-1*.
	• <CRYPTOMAP-NAME> – Enter the crypto map name (should not exceed 32 characters in length).
	• <1-1000> – Specifies the crypto map entry sequence number between 1 - 1000
	  • ipsec-isakmp – Configures IPSec w/ISAKMP. This option uses *Internet Key Exchang*e (IKE) to establish IPSec SAs to protect traffic specified by this crypto map entry.
	  • ipsec-manual – Configures IPSec w/manual keying. This option does not use IKE to establish IPSec SAs.
	  • {dynamic} – Dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration
	
	Note: The crypto map entry sequence number ranks multiple crypto map entries within a crypto map set. In a crypto map set, a map entry with lower sequence number has higher priority and is evaluated before a map entry with higher sequence number.

pki [authenticate|enroll| export|import| trustpoint]	Configures certificate parameters. The *Public Key Infrastructure* (PKI) is a protocol that creates encrypted public keys using digital certificates from certificate authorities. PKI ensures each online party is who they claim to be.
	• authenticate <TRUSTPOINT-NAME> [terminal|<URL>] – Authenticates and imports CA certificate
	• enroll <TRUSTPOINT-NAME> [request|self-signed] – Generates certificate request or selfsigned certificate for the specified trustpoint
	• export [request|trustpoint] – Exports trustpoint related configuration
	• trustpoint <TRUSTPOINT-NAME> – Creates and configures a trustpoint
	  • terminal – Copies and pastes enrollment mode
	  • request – Certificate request mode of enrollment
	  • self-signed – Selfsigned mode of enrollment
	  • trustpoint – Trustpoint configuration

Usage Guidelines

Use `crypto pki` with different parameters to configure trustpoint and its parameters. Use a crypto key to configure RSA key pairs.

Example

```
RFS7000(config)#crypto pki ?
  authenticate  Authenticate and import CA Certificate
  enroll        Enroll
  export        Export
  import        Import
  trustpoint    Define a CA trustpoint

RFS7000(config)#crypto pki trustpoint ?
```

```
  WORD  Trustpoint Name

RFS7000(config)#crypto pki trustpoint Test
RFS7000(config-trustpoint)#?
Trustpoint Config commands:
  clrscr        Clears the display screen
  company-name  Company Name(Applicable only for request)
  email         email
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  fqdn          Domain Name Configuration
  help          Description of the interactive help system
  ip-address    Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Challenge Password(Applicable only for request)
  rsakeypair    Rsa Keypair to associate with the trustpoint
  service       Service Commands
  show          Show running system information
  subject-name  Subject Name is a collection of required parameters to
                configure a trustpoint.

RFS7000(config-trustpoint)#

RFS7000(config)#crypto map cryptomap1 1 ipsec-isakmp dynamic
RFS7000(config-crypto-map)#?
Crypto Map Config commands:
  clrscr   Clears the display screen
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  match    Match values
  no       Negate a command or set its defaults
  service  Service Commands
  set      Set values for encryption/decryption
  show     Show running system information

RFS7000(config-crypto-map)#
```

5.1.13 do

Global Configuration Commands

Use this command to run commands from either the User Exec or Priv Exec mode.

Syntax

```
do (command of other mode)
```

Parameters

None

Example

```
RFS7000(config)#do ping 157.235.208.69
PING 157.235.208.69 (157.235.208.69): 100 data bytes
128 bytes from 157.235.208.69: icmp_seq=0 ttl=64 time=0.1 ms
128 bytes from 157.235.208.69: icmp_seq=1 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=2 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=3 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=4 ttl=64 time=0.0 ms

--- 157.235.208.69 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
RFS7000(config)#
```

NOTE In the example above, `ping` is a PRIV EXEC command.

5.1.14 end

Global Configuration Commands

Use this command to end the current mode and change to the Exec mode.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config)#end

RFS7000#?
Priv Exec commands:
  acknowledge    Acknowledge alarms
  archive        Manage archive files
  autoinstall    autoinstall configuration command
  cd             Change current directory
  ........................................
  ........................................
```

5.1.15 errdisable

Global Configuration Commands

Use this command to enable the timeout mechanism for the port. With errdisable enabled, the switch on detecting an error situation on the port, automatically shuts it down, and no traffic is sent or received on the port.

Syntax

```
errdisable [recovery] [cause (bpduguard)|interval <10-1000000>]
```

Parameters

recovery	Enables the timeout mechanism for the port to be enabled back
cause (bpduguard)	Specifies the reason for errdisable • bpduguard – Recovers from errdisable due to BPDU guard violation
interval <10-1000000>	Sets the interval after which port shall be enabled • <10-1000000> – Specify the errdisable-timeout interval between 10 - 1000000 seconds.

Usage Guidelines

Use a `[no]` command with the errdisable parameter to disable the bridge timeout mechanism for the port.

Example

```
RFS7000(config)#errdisable recovery interval 100
RFS7000(config)#

RFS7000(config)#errdisable recovery cause bpduguard
RFS7000(config)#

RFS7000(config)#no errdisable recovery cause bpduguard
RFS7000(config)#
```

5.1.16 firewall

Global Configuration Commands

Use this command to configure firewall parameters.

Syntax

```
firewall [802.2-encapsulation|clamp|dhcp-snoop-conflict-detection|dhcp-snoop-conflict-
logging|enable|flow|virtual-defrag|vlan-stacking]

firewall 802.2-encapsulation [permit]
firewall clamp [path-mtu|tcp-mss]
firewall dhcp-snoop-conflict-detection [disable]
firewall dhcp-snoop-conflict-logging [disable]
firewall enable
firewall flow timeout [icmp <1-32400>|other <1-32400>|tcp|udp <1-32400>]
firewall flow timeout tcp [close-wait|established|reset|setup] [<1-32400>]

firewall virtual-defrag [enable|max-defrags-per-host <1-32>|
max-defrags-per-dgram <2-8192>|min-1st-frag-length <8-1500>]
firewall vlan-stacking [permit]
```

Parameters

802.2-encapsulation [permit]	Allows 802.2p packet encapsulation that can bypass the firewall. Enabling this option is not recommended by Motorola Solutions.
clamp [path-mtu|tcp-mss]	Configures wireless firewalls • path-mtu – Limits discovered path MTU • tcp-mss – Limits TCP to inner path MTU. Enabling this option is not recommended by Motorola Solutions
dhcp-snoop-conflict-detection [disable]	Detects conflicts during IP address to MAC address mapping (based on DHCP snoop table) • disable – Disables packet drop based on conflict detection
dhcp-snoop-conflict-logging [disable]	Detects conflicts during IP address to MAC address mapping (based on DHCP snoop table) • disable – Disables logging based on conflict detection
enable	Enables firewalls

flow timeout [icmp <1-32400>| other <1-32400>| tcp <OPTION> <1-32400>| udp <1-32400>]	Configures firewall timeout for the following flow types:
	• icmp <1-32400> – Sets ICMP flow timeout value between 1 - 32400 seconds
	• other <1-32400> – Sets timeout value for other flow types between 1 - 32400 seconds
	• tcp [close-wait|established|reset|setup] <1-32400> – Sets timeout for the following TCP flow types:
	  • close-wait – CLosed TCP flow
	  • established – Established TCP flow
	  • reset – Reset TCP flow
	  • setup – Opening TCP flow

virtual-defrag [enable| max-defrags-per-host| max-frags-per-dgram| min-1st-frag-length]	Sets IPv4 virtual defragmentation parameters • enable – Enables IPv4 virtual defragmentation. Enabling of this option is recommended by Motorola Solutions. • max-defrags-per-host <1-32> – Sets the maximum active defragments allowed per host between 1 - 32 • max-frags-per-dgram <2-8129> – Sets the maximum fragments allowed per datagram between 2 - 8129 • min-1st-frag-length <8-1500> – Sets the minimum fragment length of the first fragment between 8 - 1500
vlan-stacking [permit]	Allows 802.1q VLAN stacking that can bypass the firewall. Enabling this option is not recommended by Motorola Solutions.

Example

```
RFS7000(config)#firewall clamp tcp-mss
RFS7000(config)#

RFS7000(config)#firewall virtual-defrag enable
RFS7000(config)#

RFS7000(config)#show firewall config
Wireless firewall: enabled
  IPv4 virtual defragmentation: enabled
  IPv4 TCP MSS clamping: enabled
  IPv4 path-MTU clamping: disabled
  802.2 encapsulations: denied
  802.1q vlan stacking: denied
RFS7000(config)#
```

5.1.17 hostname

Global Configuration Commands

Use this command to define the system's network name.

Syntax

```
hostname [<WORD>]
```

Parameters

<WORD>	Configures this system's network name

Example

```
RFS7000(config)#hostname Eldorado
Eldorado(config)#
```

5.1.18 interface

Global Configuration Commands

Use this command to configure a selected interface. This command is used to enter the interface configuration mode for the specified physical/ *Switch Virtual Interface* (SVI) interface. If the VLANx (SVI) interface does not exist, it is automatically created.

NOTE The interface mode leads to the `config-if` instance. For additional information, see *Interface Config commands on page 12-1*.

The prompt changes from `RFS7000(config)#` to `RFS7000(config-if)#`

Syntax

```
interface [<IFNAME>|ge <1-4>|me1|sa <1-4>|vlan <1-4094>]
```

Parameters

<IFNAME>	The interface name
ge <1-4>	Configures a GigabitEthernet interface. Select an interface index between 1 - 4.
me1	Configures a FastEthernet interface
sa <1- 4>	Configures a StaticAggregate interface. Select an interface index between 1 - 4.
vlan <1-4094>	Configures a VLAN interface. Select an interface index between 1 - 4094.

Usage Guidelines

Use `[no] interface <interface-name>` to delete the specified SVI. Valid interfaces include all VLANx interfaces.

Example

```
RFS7000(config)#interface me1
RFS7000(config-if)#

RFS7000(config)#interface ge 3
RFS7000(config-if)#

RFS7000(config)#interface sa 2
RFS7000(config-if)#

RFS7000(config)#interface vlan 400
RFS7000(config-if)#
```

5.1.19 ip

Global Configuration Commands

Use this CLI command to configure a selected *Internet Protocol* (IP) component.

NOTE Use an `ip access-list extended` command to move to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Config Commands on page 14-1*.

Use an `ip access-list standard` command to move to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Config Commands on page 15-1*.

Use an `ip dhcp pool (pool name)` command to move to the **`(config-dhcp)`** instance. For additional information, see *DHCP Config Commands on page 17-1*.

Syntax

```
ip [access-list|default-gateway|dhcp|domain-lookup|domain-name|dos|http|http-https|
  igmp|local|name-server|nat|route|routing|ssh]

ip access-list [extended|standard]
ip access-list extended [<100-199>|<2000-2699>|<ACL-NAME>]
ip access-list standard [<1-99>|<1300-1999>|<ACL-NAME>]

ip default-gateway <A.B.C.D>

ip dhcp [bootp|class|excluded-address|option|ping|pool]

ip dhcp bootp [ignore]

ip dhcp class <CLASS-NAME>

ip dhcp excluded-address [<LOW-IP-ADDRESS>] {<HIGH-IP-ADDRESS>}

ip dhcp option <option-name> <option-code> [ascii|ip]

ip dhcp ping [timeout <1-10>]ip dhcp pool <pool-name>

ip domain-lookup

ip domain-name <domain-name>

ip dos [ascend|bcast-mcast-icmp|chargen|enable|fraggle|ftp-bounce|
  invalid-protocol|option-route|router-advt|router-solicit|smurf|snork|
  tcp-intercept|tcp-max-incomplete|twinge]ip dos [ascend|bcast-mcast-icmp|chargen|
  fraggle|ftp-bounce|invalid-protocol|option-route|
  route-advt|router-solicit|smurf|snork|tcp-intercept|twinge]
  [<0-8>|alerts|critical|debugging|emergencies|errors|informational|none|
  notifications|warnings]
ip dos enable
ip dos tcp-max-incomplete [high|low] <1-1000>

ip http [secure-server|secure-trustpoint [<TRUSPOINT-NAME>]]

ip http-https [inactivity-timeout <1-1440>|max-simultaneous-sessions-per-user <1-100>]

ip igmp [snooping] {querier|unknown-multicast-fwd|vlan}
ip igmp [snooping] {querier {address <A.B.C.D>|max-response-time <1-25>|query-interval <
  <1-18000>|timer [expiry <60-300>]|version <1-3>}}
ip igmp [snooping] {vlan [<1-4094>|<VLAN-LIST>]} {mrouter|querier|unknown-multicast-
  fwd}}

ip local [pool] [default] [low-ip-address (<A.B.C.D>)] {high-ip-address (<A.B.C.D>)}

ip name-server [<A.B.C.D>]
```

```
ip nat [inside|outside] [destination|source]
ip nat inside destination [static] <LOCAL-IP> [<1-65535>|<NAT-IP>]
ip nat inside source [LIST <ACL-NAME> [INTERFACE (<IFNAME>|vlan <1-4094>)]|
  static <LOCAL-IP> <NAT-IP>]ip route [<IP-destination-prefix>|<IP-destination-prefix/
  Mask>] <gateway-IP>

ip routing

ip ssh {port|rsa}
ip ssh {port <1-65536>}
ip ssh {rsa keypair-name (<WORD>)}
```

ip (access-list)	
access-list [extended|standard]	Use the access list parameter to enter the **ext-nacl** context and **std-nacl** context. The prompt changes to the context entered. • For additional information on Extended ACL, see *Extended ACL Config Commands on page 14-1* • For additional information on Standard ACL, see *Standard ACL Config Commands on page 15-1*.
ip (default-gateway)	
default-gateway <A.B.C.D>	Configures the IP address of the default gateway (the next-hop router) • <A.B.C.D> – The IP gateway address

ip (dhcp)	

dhcp
[bootp|class|
excluded-address
|option|ping|pool]
	Configures DHCP server parameters
	• bootp [ignore] – Defines the BOOTP specific configuration
	  • ignore – Configures the DHCP server to ignore BOOTP requests
	• class <class-name> – Defines the DHCP server class name, and enters the DHCP class configuration mode
	  • <class-name> – The DHCP class name
	• excluded-address – Prevents the DHCP server from assigning certain addresses
	  • <LOW-IP-ADDRESS> – Enter this value in case of a single IP address. In case of a range of IP addresses, this value represents the first IP in the range.
	  • <HIGH-IP-ADDRESS> – Optional. In case of a range of IP addresses, this value represents the last IP in the range.
	• option <option-name> <option-code> [ascii|ip] – Defines the DHCP server's option name
	  • <option-name> – Defines the option name
	  • <0-254> – Defines the option code between 0 - 254
	  • ascii – Specifies the option type as ASCII
	  • ip – Specifies the option type as IP address
	• ping [timeout] – Specifies the DHCP server's ping timeout value
	  • timeout <1-10 > – Specifies a ping timeout between 1 - 10 seconds
	• pool <pool-name> – Defines the DHCP server's address pool name, and enters the DHCP configuration mode

ip (domain-lookup)	
domain-lookup	Enables DNS based *name - to - address* translation on the switch
ip (domain-name)	
domain-name <domain-name>	Sets the switch's domain name • <domain-name> – Enter the domain name.

ip (dos)	
dos [ascend| bcast-mcast-icmp| chargen|fraggle| ftp-bounce| invalid-ptotocol| option-route| router-advt|router-solicit| smurf|snork| tcp-intercept| twinge]	Configures following *Denial of Service* (DoS) parameters: • ascend [log] – Enables ascend DoS check • bcas-mcas-icmp [log] – Detects broadcast/multicast ICMP traffic as DoS attacks • chargen [log] – Enables chargen DoS checks • fraggle [log] – Enables fraggle DoS checks • ftp-bounce [log] – Enables FTP bounce DoS checks • invalid-protocol [log] – Enables invalid IP protocol DoS checks • option-route [log] – Enables IP option route DoS checks • router-advt [log] – Enables ICMP router advertisement DoS checks • router-solicit [log] – Enables ICMP router solicit DoS checks • smurf [log] – Enables Smurf DoS checks • snork [log] – Enables SNORK DoS checks • tcp-intercept [log] – Enables intercept DoS checks • twinge [log] – Enables Twinge DoS attacks checks The following are common to all of the above keywords: • log – Configures log levels for the DoS parameter selected. The system provides the following logging levels: • <0-8> – Logging severity level from 0 - 8 • alerts – Immediate action needed (severity level=1) • critical – Critical conditions (severity level=2) • debugging – Debugging messages (severity level=7) • emergencies – System is unusable (severity level=0) • errors – Error conditions (severity level=3) • informational – Informational messages (severity level=6) • none – Disable logging (severity level=8) • notifications – Normal but significant conditions (severity level=5) • warnings – Warning conditions (severity level=4)
ip dos enable	Enables all DoS checks
ip dos tcp-max-incomplete [high|low] <1-1000>	Configures the maximum incomplete TCP connections • high <1-1000> – Sets a higher threshold value between 1 - 1000 • low <1-1000> – Sets a lower threshold value between 1 - 1000
ip (http)	
http [secure-server| secure-trustpoint <trustpoint-name>]	Configures *Hyper Text Transfer Protocol* (HTTP) parameters • secure-server – Sets the device to start secure *HTTP Server* (HTTPS) • secure-trustpoint <trustpoint-name> – Enter the trustpoint name used for secure connection.

ip (http-https)	

http (https) [inactivity-timeout <1-1440>| max-simultaneous-sessions-per-user <1-100>]	Modifies applet session parameters
	• inactivity-timeout <1-1440> – Sets the interval with no activity after which the applet session timeouts
	  • <1-1440> – Sets the applet timeout between 1 - 1440 minutes
	• max-simultaneous-sessions-per-user <1-100> – Sets the maximum number of applet sessions per user
	  • <1-100> – Sets the maximum number of applet sessions per user between 1 - 100

ip (igmp)	

igmp snooping {querier| unknown-multicast-fwd| vlan}	Configures following IGMP snooping parameters:
	• querier {address|max-response-time|query-interval|-timer|version} – Optional. Configures IGMP querier settings
	  • address <A.B.C.D> – Optional. Sets the IGMP querier source IP address
	  • max-response-time <1-25> – Optional. Sets the IGMP querier maximum repsonse time between 1 - 25 seconds
	  • query-interval <1-180000> – Optional. Sets the IGMP querier query interval time between 1 - 18000 seconds
	  • timer [expiry <60-300>] – Optional. Sets the IGMP other querier expiry time between 60 - 300
	  • version <1-3> – Optional. Sets the IGMP verison between 1 - 3
	• unknown-multicast-fwd – Optional. Forwards packets from unregistered multicast servers
	• vlan [<1-4094>|vlan] {mrouter|querier|unknown-multicast-fwd} – Optional. Sets the VLAN to use for IGMP snooping
	  • <1-4094> – Select a single VLAN ID between 1 - 4094.
	  • <VLAN-LIST> – Specify a list of VLAN IDs (for example, 1,2,3 or a range 3-7).
	  • mrouter [interface|learn] – Optional. Sets multicast router configuration
	  • interface <list> – Can be a single or a list of GigabitEthernet interfaces (for example, ge1,ge2)
	  • learn [pim-dvmrp] – Sets the multicast switch learning PIM-DVMRP protoco
	  • querier {address|max-response-time|timer|version} – Optional. Sets IGMP querier settings for the selected VLAN interface
	  • unknown-multicast-fwd – Optional. Allows forwarding of packets from unregistered multicast servers for this VLAN interface

ip (local)	
local pool default [low-ip-address <A.B.C.D>] {high-ip-address <A.B.C.D>}	Configures the range of IP addresses assigned to VPN client using mode-config or IPSec with L2TP • pool [default] – Sets the pool tag as default • low-ip-address <A.B.C.D> – Sets the lowest IP address in the range • high-ip-address <A.B.C.D> – Optional. Sets the highest IP address in the range
ip (name-server)	
name-server	Specify the DNS server for the DHCP client. A maximum of 6 name servers can be configured. Servers are tried in the order entered • <A.B.C.D> – The DNS server IP address

ip (nat)	

nat	Configures following *Network Address Translation* (NAT) parameters:
	Syntax
	`ip nat <inside | outside> destination (static)|source <access-list name> interface <interface name>`
	• <*inside*|*outside*> – Defines the interface as private (inside) or public (external). NAT translations refer to this keyword to identify translations applied to incoming packets on an interface. Refer to *ip on page 12-10* for details on marking an interface as private (inside) or public (external).
	• destination (static <A.B.C.D) – Use the keyword `destination` to add a destination address translation. Use the key word `static` to specify local global mapping.
	• source list <access-list name> – Use the keyword `source` to add a source address translation. Use the keyword `list` (access list) to specify the traffic for NAT. This NAT is the source IP address of the traffic matching the access list.
	• interface <interface name> overload– Public or outgoing interface name. The source IP address of the traffic gets translated to the IP address of the selected interface.
	Note: Use this command to configure port NAT.
	Syntax
	`ip nat <inside | outside> destination (static) |source <access-list name> interface <interface name>`
	• <*inside*|*outside*> – Defines the interface as private (inside) or public (external). NAT translations refer to this keyword to identify translations applied to incoming packets on an interface. Refer to *ip on page 12-10* for details on marking an interface as private (inside) or public (external).
	• source list <access-list name> – Use the keyword `source` to add a source address translation. Use the keyword `list` (access list) to specify the traffic for NAT. This NAT is the source IP address of the traffic matching the access list.
	• interface <interface name> overload– Public or outgoing interface name. The source IP address of the traffic gets translated to the IP adress of the selected interface.
	Note: Use this command to configure port NAT.

ip (route)	
route	Adds a static route entry in the routing table • <IP-DESTINATION-PREFIX> – IP destination prefix. Adds a static route entry in the IP routing table • <IP-DESTINATION-PREFIX/MASK> – Mask for the IP destination prefix. Adds a static route entry in the IP routing table • <gateway-ip> – The IP address of the next hop used to reach the detsination
ip (routing)	
routing	Turns on IP routing
ip (ssh)	
ssh {port|rsa}	Configures the *Secured Shell* (SSH) server • port <1-65535> – Optional. Configures the listening port between 1 - 65536 • rsa – Optional. Configures RSA encryption parameters • keypair-name – Configures a RSA keypair used for encryption • <WORD> – The RSA keypair name

Usage Guidelines 1

By using the `ip access-list` parameter you enter the following contexts:

- ext-nacl — Extended ACL. For more details see *Extended ACL Config Commands on page 14-1*.
- std-nacl — Standard ACL. For more details see *Standard ACL Config Commands on page 15-1*.
- dhcp – DHCP server instance. For more details see *DHCP Config Commands on page 17-1*.
- dhcpclass – DHCP user class instance. For more details see *DHCP Server Class Config Commands on page 18-1*
- Use *clear* command to clear the IP DHCP binding.

NOTE To delete Standard/Extended and MAC ACL use **`no access-list <access-list name>`** under the *Global Config* mode.

Network Address Translation (NAT) allows a single device to act as a gateway for internal LAN clients. It translates the clients internal network IP addresses into the IP address of the NAT enabled device.

RFS7000 supports port NAT and static NAT.

- Static NAT allows host on a private network and is accessible through internet using public IPs.
- Static NAT assigns a public IP to a host on a private network. It allows a host on a public network to communicate with the host on the private network, using its public IP.
- Port NAT maps multiple local addresses to a single global address and dynamic port numbers.

Use `ip nat inside` to mark VLAN interfaces as an inside interface. The keyword `inside` defines the VLAN interface as internal interface. This command is used in the `(config-if)` mode, check *ip on page 12-10* for more details.

Usage Guidelines 2

Follow the steps below to create a DHCP User Class:

1. Create a DHCP class named **RFS7000DHCPclass**. RFS7000 supports a maximum of 32 DHCP classes.

```
RFS7000(config)#ip dhcp class RFS7000DHCPclass
RFS7000(config-dhcpclass)#
```

2. Create a USER class named **MC800**. The privilege mode changes to `(config-dhcpclass)`. RFS7000 supports a maximum of 8 Users classes per DHCP class.

```
RFS7000(config-dhcpclass)#option user-class MC800
RFS7000(config-dhcpclass)#
```

3. Create a Pool named **WID**, using `(config)#` mode.

```
RFS7000(config)#ip dhcp pool WID
RFS7000(config-dhcp)#
```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports association of only 8 DHCP classes with a pool.

```
RFS7000(config-dhcp)#class RFS7000DHCPclass
RFS7000(config-dhcp-class)#
```

5. The switch leads you to a new mode (config-dhcp-class). Use this mode to add an address range used for the DHCP class, associated with the pool.

```
RFS7000(config-dhcp-class)#address range 11.22.33.44
```

Example

The example below creates a named extended IP access list.

```
RFS7000(config)#ip access-list extended TestACL
RFS7000(config-ext-nacl)#
```

The example below creates a named standard IP access list.

```
RFS7000(config)#ip access-list standard TestStdACL
RFS7000(config-std-nacl)#
```

The example below creates a static NAT translation.

```
RFS7000(config)#ip nat inside destination static 1.1.1.1 2.2.2.2
RFS7000(config)#
```

The example below creates a DHCP pool.

```
RFS7000(config)#ip dhcp pool TestPool
RFS7000(config-dhcp)#
```

The example below creates a DHCP class.

```
RFS7000(config)#ip dhcp class TestDHCPclass
RFS7000(config-dhcpclass)#
```

5.1.20 license

Global Configuration Commands

Use this command to add a license to a feature.

Syntax

```
license <WORD> <LINE>
```

Parameters

<WORD>	Enter the feature name to add to the license.
<LINE>	Enter the license key.

Example

```
RFS7000(config)#show licenses
Serial Number 6283529900020
  feature          license string license value  usage
  AP                    256            4

RFS7000(config)#
```

5.1.21 line

Global Configuration Commands

Use this command to configure the terminal line.

NOTE The `line` command moves to the **`(config-line)`** instance.

Syntax

```
line [console <0-0>|vty <0-871> {<0-871>}]
```

Parameters

console <0-0>	Sets the primary terminal line to 0
vty <0-871> {0-871}	Sets the virtual terminal first line to a value between 0 - 871 • {0-871} – Optionally, sets the last line number between 0 - 871

Example

```
RFS7000(config)#line console 0
RFS7000(config-line)#

RFS7000(config)#line vty ?
  <0-871>  First Line number

RFS7000(config)#line vty 0 ?
  <0-871>  Last Line number
  <cr>

RFS7000(config)#line vty 0 871
RFS7000(config-line)#

RFS7000(config-line)#?
Line configuration commands:
  clrscr         Clears the display screen
  end            End current mode and change to EXEC mode
  exec-timeout   Set the EXEC timeout
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  login          Enable password checking
  no             Negate a command or set its defaults
  privilege      Change privilege level for line
  service        Service Commands
  show           Show running system information

RFS7000(config-line)#
```

5.1.22 local

Global Configuration Commands

Use this command to set the username and password for local user authentication.

Syntax

```
local username <USER-NAME> password [0 <passowrd>|2 <passowrd>|<passowrd>]
```

Parameters

username <USER-NAME>	Enter local user name. The username can be a string of up to 64 characters.
password	Enter local user password. The password can be a string of 8 - 21 characters. • 0 <password> – Indicates an unencrypted password • 2 <password> – Indicates encrypted password • <password> – User defined password

Example

```
RFS7000(config)#local username SuperAdmin password Superuser
RFS7000(config)#
```

5.1.23 logging

Global Configuration Commands

Use this command to modify message logging facilities.

Syntax

```
logging [aggregation-time|buffered|console|facility|host|monitor|on|snmp-set|syslog]

logging aggregation-time <1-60>

logging [buffered|console|monitor|syslog] {<0-7>|alerts|critical|debugging|
  emergencies|errors|informational|notifications|warnings}

logging facility [local0|local1|local2|local3|local4|local5|local6|local7]

logging host <A.B.C.D>

logging on

logging snmp-set enable
```

Parameters

aggregation-time <1-60>	Sets number of seconds (between 1 - 60) for aggregating repeated messages
buffered	Sets the buffered logging level • <0-7> – Logging severity level • alerts – Immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7) • emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)
console	Sets the console logging level • <0-7> – Logging severity level • alerts – Immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7) • emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)

facility	Syslog facility in which log messages are sent • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7
host <A.B.C.D>	Configures the remote host to receive log messages • <A.B.C.D> – Enter remote host's IP address.
monitor	Sets the terminal line logging level • <0-7> – Logging severity level • alerts – Immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7)emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)
on	Enables the logging of system messages
snmp-set	Enables logging of SNMP set request
syslog	Sets the syslog servers logging level • <0-7> – Logging severity level • alerts – Immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7) • emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)

Example

```
RFS7000(config)#logging aggregation-time 20
RFS7000(config)#
```

5.1.24 mac

Global Configuration Commands

Use this command to configure MAC access lists.

Syntax

```
mac access-list [extended (<WORD>)]
```

Parameters

access-list (extended <name>)	Enter extended MAC ACL name.

Usage Guidelines

To delete a Standard/Extended or MAC ACL, use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
RFS7000(config)#mac access-list extended Test1
RFS7000(config-ext-macl)#
```

NOTE By using the `mac access-list` parameter, the following context is supplied:

- ext-macl — Extended MAC ACL. For additional information, see *MAC Extended ACL Config Commands on page 16-1*

5.1.25 mac-address-table

Global Configuration Commands

Use this command to configure MAC adress table.

Syntax

```
mac-address-table aging-time [0|<10-1000000>]
```

Parameters

aging-time [0|<10-1000000>]	The duration for which a learned MAC address will persist after last update • 0 – Disables aging • <10-1000000> – Specifies the aging time between 10 - 1000000 seconds

Example

```
RFS7000(config)#mac-address-table aging-time 100
RFS7000(config)#
```

5.1.26 mac-name

Global Configuration Commands

Use this command to configure a MAC name for a specified MAC address.

Syntax

```
mac-name <MAC-ADDRESS> <LINE>
```

Parameters

<MAC-ADDRESS>	Specify the MAC address in the AA-BB-CC-DD-EE-FF format.
<LINE>	Specify the name to be configured with the specified MAC address. **Note:** The name should confirm to the DNS naming convention.

Example

```
RFS7000(config)#mac-name 11-22-33-44-55-66 TEST1
RFS7000(config)#
```

5.1.27 management

Global Configuration Commands

Use this command to set management interface properties.

Syntax

Parameters`management [secure]`

secure	Limits local access (Web) to the management interface

Example

```
RFS7000(config)#management secure
RFS7000(config)#
```

5.1.28 network-element-id

Global Configuration Commands

Use this command to set the system's network element ID.

Syntax

```
network-element-id <WORD>
```

Parameters

network-element-id <WORD>	Sets this system's network element ID • <WORD> – Specify the network element ID to set.

Example

```
RFS7000(config)#network-element-id TechPub1
```

5.1.29 ntp

Global Configuration Commands

Use this command to configure *Network Time Protocol* (NTP) parameters.

Syntax

```
ntp [access-group|authenticate|authentication-key|autokey|master|peer|
  server|trusted-key]

ntp access-group [peer|query-only|serve|serve-only] [<1-99>|<100-199>|<1300-1999>|
  <2000-2699>]

ntp authenticate

ntp authentication-key <key-number> [md5 [0 <LINE>|2 <LINE>|<LINE>]]

ntp autokey [client-only|host]

ntp master {<1-15>}

ntp peer <Peer-name/IP-Address> {autokey|key|prefer|version}
ntp peer <Peer-name/IP-Address> autokey {prefer (version <1-4>)}
ntp peer <Peer-name/IP-Address> key <1-65534> {prefer (version <1-4>)}
ntp peer <Peer-name/IP-Address> prefer {version <1-4>}
ntp peer <Peer-name/IP-Address> version <1-4> {prefer}

ntp server <Peer-IP-Adrress> {autokey|key|prefer|version}
ntp server <Peer-IP-Adrress> autokey {prefer (version <1-4>)}
ntp server <Peer-IP-Adrress> key <1-65534> {prefer (version <1-4>)}
ntp server <Peer-IP-Adrress> prefer {version <1-4>}
ntp server <Peer-IP-Adrress> version <1-4> {prefer}

ntp trusted-key <1-65534>
```

Parameters

ntp (acces-group)	

access-group [peer|query-only|serve| serve-only]	Configures NTP access
	• peer – Provides full access
	  • <1-99> – Standard IP access list
	  • <100-199> – Extended IP access list
	  • <1300-1999> – Standard IP access list (expanded range)
	  • <2000-2699> – Extended IP access list (expanded range)
	• query-only – Allows only control queries
	  • <1-99> – Standard IP access list
	  • <100-199> – Extended IP access list
	  • <1300-1999> – Standard IP access list (expanded range)
	• serve – Provides server and query access
	  • <1-99> – Standard IP access list
	  • <100-199> – Extended IP access list
	  • <1300-1999> – Standard IP access list (expanded range)
	  • <2000-2699> – Extended IP access list (expanded range)
	• serve-only – Provides only server access
	  • <1-99> – Standard IP access list
	  • <100-199> – Extended IP access list
	  • <1300-1999> – Standard IP access list (expanded range)
	  • <2000-2699> – Extended IP access list (expanded range)

ntp (authenticate)	
authenticate	Authenticates time sources
ntp (autehntication-key)	

authentication-key <1-65534>	Defines an authentication key for trusted time sources. Select a key number between 1 - 65534.
	• md5 – MD5 authentication
	  • 0 <LINE> – Configures unencrypted password
	  • 2 <LINE> – Configures encrypted password. Specify the password encryption secret.
	  • <LINE> – The authentication key

ntp (autokey)	
autokey [client-only|host]	Enables the NTP autokey authentication scheme • client-only – Configures the switch as a client to other trusted hosts in the autokey group • host – Configures the switch as a trusted host
ntp (master)	
master {<1-15>}	Acts as a NTP master clock • <1-15> – Optional. Sets the stratum number for the NTP master clock between 1 - 15
ntp (peer)	
peer <PEER-NAME/ IP-ADDRESS>	Configures a NTP peer • <Peer-Name/IP-Address> – Sets the name/IP address of the peer • autokey – Optional. Configures autokey peer authentication scheme • key – Optional. Configures peer authentication key • prefer – Optional. Configures this peer as the preferred peer • version – Optional. Specifies the NTP version configured between 1 - 4
ntp (server)	
server <PEER-IP-ADDRESS>	Configures a NTP serve.<PEER-IP-ADDRESS> – The IP address of the peer only • autokey – Optional. Configures autokey peer authentication scheme • key – Optional. Configure peer authentication key. • prefer – Optional. Configures this peer as the preferred peer • version – Optional. Specifies the NTP version configured between 1 - 4.
ntp (trusted-key)	
trusted-key <1-65534>	Configures key numbers for trusted time sources between 1- 65534

Example

```
RFS7000(config)#ntp peer ?
  WORD  Name/IP address of peer

RFS7000(config)#ntp peer TestPeer ?
  autokey  Configure autokey peer authentication scheme
  key      Configure peer authentication key
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer autokey ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer autokey prefer ?
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer autokey prefer version ?
  <1-4>  NTP version number
```

```
RFS7000(config)#ntp peer TestPeer autokey prefer version 3
RFS7000(config)#

RFS7000(config)#ntp peer TestPeer key ?
  <1-65534>  Peer key number

RFS7000(config)#ntp peer TestPeer key 20 ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer key 20 prefer ?
  version  Configure NTP version
  <cr>
```

5.1.30 prompt

Global Configuration Commands

Use this command to configure and set the system prompt.

Syntax

Parameters`prompt <LINE>`

<LINE>	Enter the new prompt displayed by the switch with the optional modifiers mentioned below: • %% – Percent sign • %h – Hostname • %m – Current configuration mode • %n – CLI line • %p – Privilege mode sign • %s – Space • %t – Tab • %A – Date and time in ASCII format • %D – Date in MM/DD/YY format • %N – Newline • %T – Time in hh:mm:ss format

Example

```
RFS7000(config)#prompt ?
  LINE  String + optional modifiers below
        %%      Percent sign
        %h      Hostname
        %m      Current configuration mode
        %n      Cli line
        %p      Privilege mode sign
        %s      Space
        %t      Tab
        %A      Date and time in ASCII format
        %D      Date in MM/DD/YY format
        %N      Newline
        %T      Time in hh:mm:ss format


RFS7000(config)#prompt NobleMan %h
NobleMan RFS7000
```

5.1.31 radius-server

Global Configuration Commands

Use this command to enter the RADIUS server mode. The system prompt changes from the default config mode to RADIUS server mode.

NOTE `radius-server` **`local`** mode moves to the radius-server context. For more details see *RADIUS Configuration Commands on page 19-1*

Syntax

```
radius-server [host|key|local|retransmit|timeout]
radius-server host [A.B.C.D] {key|retransmit|timeout}
radius-server key [0 <LINE>|2 <LINE>|<LINE>]
radius-server local
radius-server retransmit <0-100>
radius-server timeout <1-1000>
```

Parameters

host	Configures a specific RADIUS server • <A.B.C.D> – Specify the RADIUS server's IP address to configure. (uses the default port 1812)
key	Configures the encryption key shared with the RADIUS servers • 0 <LINE> – Password specified as UNENCRYPTED • 2 <LINE> – Password is encrypted with password-encryption secret • <LINE> – Text of shared key (up to 127 characters in length)
local	Configures local RADIUS server parameters. This takes you to a new **`config-radius-server`** context. Refer to *page 19-1* for more details.
retransmit <0-100>	Specifies the number of retries to the active RADIUS server • <0-100> – Select the number of retries for a transaction between 0 - 100 (default is 3).
timeout <1-1000>	Configures the wait time for a RADIUS server reply • <1-1000> – Select a value between 1 - 1000 (default 5 seconds).

Usage Guidelines

RADIUS server host is used to configure RADIUS server details. These details are required for management user authentication if AAA authentication has been defined as RADIUS.

Example

```
RFS7000(config)#radius-server local
RFS7000(config-radsrv)#
```

5.1.32 ratelimit

Global Configuration Commands

Use this command to enable ratelimit logging.

Syntax

```
ratelimit [arp|bcast|mcast|ucast] [log] [<0-7>|alerts|critical|debugging|
  emergencies|errors|informational|notifications|warnings]
```

Example

arp [log]	Enables ARP packet ratelimit logging
bcast [log]	Enables broadcast packet ratelimit logging
mcast [log]	Enables multicast packet ratelimit logging
uncast [log]	Enables unicast packet ratelimit logging
log [<0-7>|alerts|critical| debugging|emergencies| errors|informational| notifications|warnings]	The following logging parameters are common to the 'arp'. 'bcast', 'mcast', 'uncast' keywords: • <0-7> – Select a logging severity logging level between 0 -7 • alerts – Immediate action needed (severity level = 1) • critical – Critical conditions (severity level = 2) • debugging – Debugging message (severity level = 7) • emergencies – System is unusable (severity level = 0) • errors – Error conditions (severity level = 3) • informational – Informational messages (severity level = 6) • notifications – Normal but significant conditions (severity level = 5) • warnings – Warning conditios (severity level = 4)

```
RFS7000(config)#ratelimit arp log alerts
RFS7000(config)#
```

5.1.33 redundancy

Global Configuration Commands

Use this command to configure redundancy group parameters.

Syntax

```
redundancy [auto-revert|auto-revert-period|critical-resource-ip|dhcp-server|
  discovery-period|dynamic-ap-load-balance|enable|group-id|handle-stp|
  heartbeat-period|hold-period|interface-ip|manual-revert|member-ip|mode]

redundancy auto-revert [enable]
redundancy auto-revert-period <1-1800>
redundancy critical-resource-ip <A.B.C.D>
redundancy dhcp-server [enable]
redundancy discovery-period <10-60>
redundancy dynamic-ap-load-balance [enable|per-ap-mu-threshold <1-512>|
schedule-interval <1-366>|schedule-start-time|trigger (runtime|schedule)]
redundancy enable
redundancy group-id <1-65535>
redundancy handle-stp [enable]
redundancy heartbeat-period <1-255>
redundancy hold-period <13-255>
redundancy interface-ip [<A.B.C.D>]
redundancy manual-revert
redundancy member-ip [<A.B.C.D>]
redundancy mode [primary|standby]
```

Parameters

auto-revert [enable]	Enables auto-revert
auto-revert-period <1-1800>	Sets the redundancy auto-revert delay interval • <1-1800> – Specify the auto-revert delay intervalbetween 1 - 1800 minutes (default is 5 minutes).
critical-resource-ip <A.B.C.D>	Sets the critical resource IP address • <A.B.C.D> – Specify the e critical resource IP address.
dhcp-server [enable]	Enables DHCP redundancy protocol
discovery-period <10-60>	Sets the redundancy discovery interval • <10-60> – Specify the discovery time between 10 -60 seconds (default is 30 seconds).

dynamic-ap-load-balance [enable| per-ap-mu-threshold| schedule-interval| schedule-start-time| trigger]	Configures dynamic AP load balance parameters
	• enable – Enables dynamic AP load balancing
	• per-ap-mu-threshold <1-512> – Specifies per AP mobile unit threshold count between 1 - 512
	• schedule-interval – Schedules dynamic AP load balance interval between 1 - 366 days
	• schedule-start-time – Schedules dynamic AP load balance start time
	  • HH:MM – Specify the start time in the 24-hour format (hours <0-23> followed by minutes <0-59>).
	  • <1-31> – Specify the day of the month.
	  • <1-12> – Specify the month.
	  • <2008-2035> – Specify the year between 2008 - 2035.
	• trigger [runtime|schedule] – Specifies the type of trigger for AP load balancing
	  • runtime – Sets the trigger based on runtime trigger
	  • schedule – Sets the trigger at the configured schedule time

enable	Enables the redundancy protocol
group-id <1-65535>	Sets the redundancy/cluster group ID • <1-65535> – Specify the redundancy group ID between 1 - 65535.
handle-stp [enable]	Delays the redundancy protocol state machine exec, considering STP • enable – Sets the handle-stp value as true
heartbeat-period <1-255>	Sets the redundancy heartbeat interval.The `heartbeat-period` must always be less than the `hold-period`. • <1-255> – Specify the heartbeat interval between 1 - 255 seconds (default is 5 seconds).
hold-period <3-255>	Sets the redundancy hold interval • <3-255> – Specify the hold interval between 3 - 255 seconds (default is 15 seconds).
interface-ip <A.B.C.D>	Sets the redundancy interface IP address. • <A.B.C.D> – Specify the IP address of the switch.
manual-revert	Reverts standby to non-active mode
member-ip <A.B.C.D>	Adds a member to this redundancy group • <A.B.C.D> – Specify the IP address of the member.
mode [primary|standby]	Sets the switch mode to either primary or standby • primary – Defines mode as primary • standby – Defines mode as standby

Example

```
RFS7000(config)#redundancy discovery-period 20
RFS7000(config)#

RFS7000(config)#redundancy handle-stp enable
RFS7000(config)#

RFS7000(config)#redundancy heartbeat-period 20
RFS7000(config)#

RFS7000(config)#redundancy hold-period 25
RFS7000(config)#

RFS7000(config)#redundancy mode primary
RFS7000(config)#
```

5.1.34 remote-login

Global Configuration Commands

Use this command to configure remote login parameters.

Syntax

```
remote-login [max-allowed-failure] <1-1024>
```

Parameters

max-allowed-failure <1-1024>	Sets the maximum allowed login attempts failures before remote login is disabled • <1-1024> – Specify the number of failed login attempts between 1 -1024.

Example

```
RFS7000(config)#remote-login max-allowed-failure 100
RFS7000(config)#
```

5.1.35 role

Global Configuration Commands

Use this command to configure a role and its parameters.

Syntax

```
role [<ROLE-NAME>|assignment]
role <ROLE-NAME> <1-10001>
role assignment immediate enable
```

Parameters

<ROLE-NAME> <1-10001>	Configures the role name • <ROLE-NAME> – Specify a role name to configure (should not exceed 20 characters). • <1-1001> – Set a role priority between 1 - 10001. This is in case of multiple role match, then the role with the lowest priority is selected. Will take you to the **config-role** mode.
assignment [immediate] [enable]	Assigns a role to a mobile unit • immediate – Reapplies roles to mobile unit after approximately 30 seconds, if an existing role is edited or a new role is created • enable – Enables immediate role assignment and triggers role-revaluation

Example

```
RFS7000(config)#role SuperAdmin 2
RFS7000(config-role)#?
Role Config commands:
  ap-location          ap location configuration
  authentication-type  Type of Authentication
  clrscr               Clears the display screen
  encryption-type      Type of Encryption
  end                  End current mode and change to EXEC mode
  essid                essid configuration
  exit                 End current mode and down to previous mode
  group                group configuration
  help                 Description of the interactive help system
  ip                   Internet Protocol (IP)
  mac                  MAC ACL commands
  mu-mac               mu mac address configuration
  no                   Negate a command or set its defaults
  service              Service Commands
  show                 Show running system information

RFS7000(config-role)#

RFS7000(config)#role assignment immediate enable
RFS7000(config)#
```

5.1.36 rtls

Global Configuration Commands

Use this command to configure locationing mode parameter settings. This command will take you to the **config-rtls** mode.

Syntax

```
rtls
```

Parameters

None

Example

```
RFS7000(config)#rtls
RFS7000(config-rtls)#?
Locationing Config commands:
  aeroscout  aeroscout configuration parameters
  ap         Access port coordinate configuration
  clrscr     Clears the display screen
  ekahau     ekahau configuration parameters
  end        End current mode and change to EXEC mode
  exit       End current mode and down to previous mode
  help       Description of the interactive help system
  no         Negate a command or set its defaults
  service    Service Commands
  show       Show running system information
  site       Site configurations
  sole       Configure Location Engine Parameters
  switch     Configure switch parameters

RFS7000(config-rtls)#
```

5.1.37 service

Global Configuration Commands

Use this command to retrieve system data (tables, log files, configuration, status and operation) for use in debugging and problem resolution.

Syntax

```
service [advanced-vty|dhcp|diag|pm|radius|redundancy|set|show|terminal-length|watchdog]

service advanced-vty
service dhcp

service diag [enable|limit|period]
service diag limit [buffer|fan|filesys|inodes|load|maxFDs|
  pkbuffres|procRAM|ram|routecache|temerature]
service diag period <100-30000>

service pm sys-restart

service radius {restart|test}
service radius {test [<A.B.C.D>|<WORD>] <Secret> <User-Name> <password> {<wlan>}

service redundancy [dynamic-ap-load-balance] [start]
service set [command-history <10-300>|reboot-history <10-100>|upgrade-history <10-100>]
service show [cli]
service terminal-length <0-512>
service watchdog
```

Parameters

advanced-vty	Enables the advanced mode vty interface
dhcp	Enables the DHCP server

diag [enable|limit| period <100-30000>]	Enables diagnostic service
	• enable – Enables service diagnostics
	• limit – Configures following diagnostic limits:
	  • buffer [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k] – Sets buffer usage warning limit in bytes
	  • fan <1-3> – Sets the fans speed limit for the selected fan number
	  • filesys [etc2|flash|var] – Sets file system freespace limit
	  • inodes [etc2|flash|var] – Sets file system inode limit
	  • load [01|05|15] – Sets the agregate processor load during the previous minutes, using the options provided
	  • maxFDs <0-32767> – Sets maximum number of file descriptors between 0 - 32767
	  • pkbuffers <0-65535> – Sets packet buffer head cache limit between 0 - 65535
	  • procRAM <0.0-100.0> – Sets RAM space to be used by the process between 0.0 - 100.0 percent
	  • ram <0.0-25.0> – Sets free RAM space between 0.0 - 25.0 percent
	  • routecache <0-65535> – Sets IP route cache usage limit between 0 - 65535
	  • temperature <1-6> – Sets temperature limit for the selected switch temprature sensor. A maximum of six temperature sensors can be configured.
	  • <1-6> [critical|high|low] <0.0-250.0> – Sets the temperature limit as critical, high, or low between 0.0 - 250.0
	• period <100-30000> – Sets diagnostics period between 100 - 300000 milliseconds. Default is 1000 milliseconds.

pm [sys-restart]	Enables the *Process Monitor* (PM) to restart the system when a process fails **Note:** The process restart is one count less than what is configured.

radius [restart|test]	Enables the RADIUS server
	• restart – Restarts the RADIUS server with updated configuration
	• test <A.B.C.D> <WORD> – Tests the RADIUS server with user parameters
	  • <A.B.C.D> – The RADIUS server IP address
	  • <WORD> – The RADIUS server hostname

set [command-history| reboot-history| upgrade-history]	Sets service parameters • command-history – Sets the command history size between 10 - 300 (default is 200) • reboot-history – Sets the reboot history size between 10 -100 (default is 50) • upgrade-history – Sets the upgrade history size between 10 -100 (default is 50)
show cli	Shows the CLI tree of the current mode
terminal-length <0-512>	Configures the system wide terminal length. • <0-512> – Select a value between 0 - 512. This sets the number of lines of VTY (0 means no line control).
watchdog	Enables the watchdog feature

Example

```
RFS7000(config)#service dhcp
RFS7000(config)#

RFS7000(config)#service radius restart
RFS7000(config)#

RFS7000(config)#service show cli
Global Config mode:
+-aaa
  +-authentication
    +-login
      +-default
        +-local [aaa authentication login default {none|{local|radius}}]
        +-none [aaa authentication login default {none|{local|radius}}]
        +-radius [aaa authentication login default {none|{local|radius}}]
+-access-list
  +-<1-99>
    +-deny
      +-A.B.C.D/M [access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos
<0-255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
        +-log [access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
          +-rule-precedence
            +-<1-5000> [access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7>
| tos <0-255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
        +-rule-precedence
RFS7000(config)#
```

5.1.38 show

Global Configuration Commands

Use this command to view running system information.

Syntax

```
show <display parameter>
```

Parameters

aap-wlan-acl [<1-256>|all]	Displays WLAN based ACL • <1-256> – The WLAN ID. This displays the ACL attached to the WLAN ID specified by the <1-266> value. • all – Displays ACLs attached to all WLANs
aap-wlan-acl-stats	Displays IP filtering WLAN based statistics
access-banner	Displays access banner
access-list {<1-99>| <100-199>|<1300-1999>| <2000-2699>]<WORD>}	Displays details of the specified access list • <1-99> – IP standard access list • <100-199> – IP extended access list • <1300-1999> – IP standard access list (extended range) • <2000-2699> – IP extended access list (extended range) • <WORD> – The ACL name

aclstats [access-list|vlan]	Displays ACL statistics information
	• access-list {<1-99>| <100-199>| <1300-1999>|<2000-2699>|<WORD>} – Configured access list
	  • <1-99> – IP standard access list
	  • <100-199> – IP extended access list
	  • <1300-1999> – IP standard access list (extended range)
	  • <2000-2699> – IP extended access list (extended range)
	  • <WORD> – The ACL name
	• vlan <1-4094> – The VLAN interface index between 1 - 4094

alarm-log {<1-65535>| acknowledged|all|count| new|severity-to-limit}	Displays all alarms currently in the system • <1-65535> – Displays details of the alarm specified by the <1-65535> value • acknowledged – Displays acknowledged alarms currently in the system • all – Displays all alarms currently in the system • count – Displays total alarm count currently in the system • new – Displays new alarms currently in the system • severity-to-limit – Displays all alarms with specified or higher severity
audit-log-filters	Displays audit log filter rules
autoinstall {status}	Displays autoinstall status (whether initiated or not)
boot	Displays the boot configuration

clock	Displays the system clock
commands	Displays the command lists

crypto [ipsec|isakmp|key|map|pki]	Displays encryption configuration
	• ipsec [sa|security-associaton|transformset] – Displays IPSec policy details.
	  • sa – Displays IPSec *Security Association* (SA)
	  • Security-association (lifetime) – Displays SA lifetime
	  • lifetime – Displays Security-association lifetime
	  • transformset {<WORD>} – Displays the specified transformset
	  • <WORD> – The transformset name. If no name is specified, the system displays all transformsets
	• isakmp [policy|sa] – Displays selected ISAKMP configurations
	  • policy {<1-10000>} -— Displays ISAKMP policy specified by the <1-10000> sequence number
	  • sa – Displays all crypto ISAKMP SAs
	• key [mypubkey] – Displays authentication key management
	  • mypubkey [rsa] – Displays public keys associated with the switch
	  • rsa – Displays RSA public keys
	• map [interface|tag] – Displays crypto maps
	  • interface <WORD> – Displays crypto maps for an interface
	  • <WORD> – Interface name to display crypto maps for
	  • tag <WORD> – Displays crypto maps for a given tag
	  • <WORD> – The crypto map name
	• pki [request|trustpoint] – Displays *Public Key Infrastructure* (PKI) commands
	  • request <WORD> – Displays certificate request
	  • <WORD> – The trustpoint nametrustpoint – Displays trustpoints configured and configuration

crypto-error-log	Displays crypto error log
crypto-log	Displays crypto log
debugging (mstp)	Displays debugging information outputs • mstp – Displays *Mutiple Spanning Tree Protocol* (MSTP) debugging status
dhcp [config|status]	Displays the DHCP server configuration • config – Displays DHCP server configuration • status – Displays whether DHCP server is running or not
environment	Displays environmental information

file [information|systems]	Displays filesystem information • information <FILE> – Displays specified file information • systems – Lists file systems
firewall [config|dhcp|flow]	Displays wireless firewall detailsconfig – Displays firewall configuration • dhcp (snoop-table)– DHCP basedsnoop-table – Displays snoop Table Entries • flow (timeouts) – Displays Firewall flow • timeouts – Displays wireless firewall flow timeout configuration
history	Displays the session command history
interfaces {<WORD>| ge <1-4>|me1|sa <1-4>| switchport <options>| vlan <1-4094>}	Displays a specified interface status. Select the interface type: • <WORD> – Specify the interface name. • ge <1-4> – Specify the GigabitEthernet interface index between 1 - 4. • me1 – Specifies the FastEthernet interface. • sa <1-4> – Specify the StaticAggregate interface index between 1 - 4. • switchport – Specifies a Layer2 interface • vlan <1-4094> – Specify the VLAN interface index between 1 - 4094.

ip [access-group|
access-list|arp|ddns|
dhcp|
dhcp-vendor-options|
domain-name|dos|
http|igmp|interface|
name-server|nat|route|
routing|ssh]
	Displays the *Internet Protocol* (IP) configuration
	• access-group [<Interface-name>|all|ge|me1|role|sa|vlan] – Displays ACLs. attached to an interface
	  • <interface-name> – The interface to display access-group information for
	  • all – Displays access-group information for all interfaces.
	  • ge <1-4> – Displays access-group information for the GigabitEthernet interface specified by the <1-4> value
	  • me1 – Displays access-group information for the management interface
	  • role <ROLE-NAME> – Displays access-group information for the role specified by the <ROLE-NAME> value
	  • sa <1-4> – Displays access-group information for the StaticAggregate. interface with the value <1-4>
	  • vlan <1-4094> – Displays access-group information for VLAN with ID <1-4094>
	• access-list – Lists all configured IP access lists
	• arp – Displays IP to MAC address mappings
	• ddns – Displays DDNS configuration
	  • binding –Displays DNS address bindings
	• dhcp [bindings|class|pool|sharednetwork] – Displays following DHCP server configurations:
	  • bindings – DHCP address bindings
	  • class – DHCP server class details
	  • pool – DHCP pool details
	  • sharednetwork – Shared Network
	  • manual – Static DHCP address bindings
	  • <WORD> – The class/pool name

	• dhcp-vendor-options – Displays DHCP option 43 parameters received from the DHCP server
	• domain-name – Displays default DNS domain status
	• dos – Displays following *Denial of Service* (DoS) settings:
	  • config – Displays IP DoS configuration
	  • stats – Displays IP DoS statistics
	• http [secure-server] – Displays *HyperText Transfer Protocol* (HTTP) secure server status (whether running or not), configuration status, and trustpoint details
	• igmp (snooping) – Displays the IGMP configuration
	  • snooping {mrouter|querier|vlan} – Displays the IGMP snooping configuration
	• interface {<IFNAME>|brief|vlan} – Displays the IP information of the interface
	  • <IFNAME> – The interface to display the information for
	  • brief – Displays a brief summary of IP status and configuration of the interface
	  • vlan <1-4094> – Displays the status of the VLAN for the ID <1-4094>

	• name-server – Displays the IP configuration of the specified DNS name server
	• nat [interfaces|translations] – Displays the configuration of *Network Address Translations* (NAT)
	  • interfaces – Displays the NAT configuration on the interfaces
	  • translations {inside|outside|verbose} – Displays NAT translations
	  • Inside – Inside
	  • Outside – outside
	  • destination – Destination
	  • source – Source
	  • verbose – NAT translation in real-time.
	• route {<A.B.C.D>|<A.B,C.D/M>|detail} – Displays IP routing table
	  • <A.B.C.D> – Network in the IP routing table to display
	  • <A.B.C.D/M> – IP prefix <network> <length>
	  • detail – Displays IP routing table in detail
	• routing – Displays routing status
	• ssh – Displays SSH server status and configuration

ldap [configuration]	Displays the *Lightweight Directory Access Protocol* (LDAP) server configuration
	• configuration {primary|secondary} – Specifies LDAP configuration parameters
	  • primary – Displays primary LDAP server configuration
	  • secondary – Displays secondary LDAP server configuration

licenses	Displays installed licenses details
logging	Displays logging configuration and buffer data
mac [access-group| access-list]	Displays MAC access-list assignment details • access-group – Displays MAC ACLs attached to an interface. Specify the interface to view MAC ACL • access-list – Lists MAC access lists
mac-address-table	Displays the MAC address table
mac-name	Displays the configured MAC name details
management	Displays L3 Management Interface details

mobility [event-log| forwarding|global| mobile-unit|peer| statistics]	Displays mobility parameters
	• event-log [mobile-unit|peer] – Displays event logs
	  • mobile – Displays station event-logs
	  • peer – Displays peer event-logs
	• forwarding {<AA-BB-CC-DD-EE-FF>} – Displays mobile-units in the Forwarding Plane
	  • <AA-BB-CC-DD-EE-FF> – The MAC address of the mobile unit to display
	• global – Displays Global Mobility parameters
	• mobile-unit {<AA-BB-CC-DD-EE-FF>|detail} – Displays mobile-units in the mobility database
	  • <AA-BB-CC-DD-EE-FF> – The MAC address of the mobile unit to display
	  • detail – Displays detailed information
	• peer {<A.B.C.D>|detail} – Displays mobility peers
	  • <A.B.C.D> – The IP address of peer
	  • detail – Displays detailed information
	• Statistics {<AA-BB-CC-DD-EE-FF>} – Displays mobility statistics
	  • <AA-BB-CC-DD-EE-FF> – The MAC address of the mobile unit to display

ntp [associations|status]	Displays *Network Time Protocol* (NTP) configuration • associations (detail) – Displays NTP associations. • detail – Displays NTP association details • status – Displays NTP status

password-encryption [status]	Displays password encryption status (whether enabled or not)
port [fw] [config]	Displays physical/aggregate port interface configurationfw (config) – Displays firewalls • config – Displays configurable firewall parameters
port-channel [load-balance]	Displays port channel load balancing
privilege	Displays the current privilege level
protocol-list	Displays list of protocols
radius [configuration|eap|group|nas|proxy|rad-user|trust-point]	Displays RADIUS configuration commands • configuration – Displays RADIUS server configuration parameters • eap (configuration) – Displays EAP parameters • configuration – Displays EAP configuration • group – Displays RADIUS group configuration • nas <A.B.C.D/M>– Displays client information • <A.B.C.D/M> – Specifies client IP address/mask • proxy <WORD> – Displays proxy information • <WORD> – Specifies proxy realm name • rad-user <WORD> – Displays RADIUS user information • <WORD> – The existing user name in the local RADIUS database • trust-point – Displays RADIUS trustpoint information
redundancy-group [dynamic-ap-load-balance|group|history|members]	Displays redundancy group parameters • dynamic-ap-load-balance [config] – Displays redundancy dynamic AP load balance parameters • config – Displays configuration details for dynamic AP load balance • group {config|runtime} - Displays redundancy group parameters • config – Displays configured redundancy group information • runtime – Displays runtime redundancy group information • history – Displays state transition history of the switch • members {<A.B.C.D>|brief} – Displays redundancy group members in detail • <A.B.C.D> – Specifies the IP address of the member switch • brief – Displays members in brief
role {<WORD>|mobile-units}	Displays role parameters • <WORD> – Specify an existing role to view details • mobile-units – Displays the mobile-units assigned with configured role

rtls [aeroscout|ekahau|filter|site|sole|tags|zone]	Displays information on *Real Time Locating System* (RTLS) commands
	• aeroscout – Displays aeroscout configurations
	• ekahau – Displays ekahau configurations
	• filter – Displays *Radio Frequency Identification* (RFID) tag filters
	• site – Displays site configurations
	• sole [peer|probe] – Displays SOLE configurations
	  • peer – Displays SOLE peer information
	  • probe – Displays probe information
	• tags – Displays tags/assets information
	• zone {<1-48>|detail} – Displays zone statistics

running-config {full|include-factory}	Displays the current running configuration • full – Displays full configuration • include-factory – Includes factory defaults **Note:** If the AP / MU locationing configuration has non default parameters, it shows up here.
securitymgr [event-logs]	Displays securitymgr event logs
service-list	Displays list of services
sessions	Displays current active open connections

snmp (user)	Displays SNMP engine parameters
	• user [snmpmanager|snmpoperator|snmptrap] – The SNMP user to display information for
	  • snmpmanager – Displays manager information
	  • snmpoperator – Displays operator information
	  • snmptrap – Displays trap user information

snmp-server {traps}	Displays SNMP engine parameters
	• traps {wireless-statistics} – Displays Trap enable flags
	  • wireless-statistics [mesh|mobile-unit|radio|wireless-switch|wlan] – Displays wireless-stats rate traps
	  • mesh – Displays mesh rate traps
	  • mobile-unit – Displays mobile unit rate traps
	  • radio – Displays radio rate traps
	  • wireless-switch – Displays wireless switch rate traps
	  • wlan – Displays WLAN rate traps

spanning-tree [mstp]	Displays spanning tree information
	• mst {configuration|detail|instance} – Displays MST information
	  • configuration – Displays MST configuration information
	  • detail – Displays detailed MST information
	  • instance <1-15> – Displays information for the instance ID <1-15>

startup-config	Displays contents of startup configuration
static-channel-group	Displays static channel group membership
terminal	Displays terminal configuration parameters
timezone	Displays the timezone
traffic-shape	Displays traffic shaping • config – Displays traffic shaping configuration • priority-map – Displays .1pto transmit priority map • statistics – Displays traffic shaping statistics
upgrade-status {detail}	Displays the last image upgrade status • detail – Displays last image upgrade log
users	Displays information of currently logged in users
version {verbose}	Displays software and hardware version details
virtual-ip [config|status]	Displays IP redundancy configuration and status

wireless [aap-version|ap| ap-containment| ap-detection-config| ap-images| ap-radio-config| ap-adopted| authorized-aps| channel-power| config|country-code-list| default-ap|fw|hotspot| hotspot-config| ignored-aps|known| mac-auth-local|mesh| mobile-unit|	Displays Wireless configuration commands
	• aap-version – Displays the minimum adaptive firmware version string
	• ap {<LIST>|config} – Displays tadopted access-port status<LIST> – List the MAC address of a single access-port or a list of indices for detailed information.
	  • config – Displays configured access port status
	• ap-containment [config|table]– Displays rogue AP containment parameters
	  • config – Displays rogue AP containment configuration parameters
	  • table – Displays rogue AP containment table
	• ap-detection-config – Displays detected AP configuration parameters
	• ap-images – Lists access-port images on the wireless switch
	• ap-radio-config [<MAC-Address>] – Displays AP radio configuration for the specified radio
	  • <MAC- Address> – The MAC address of the AP radio to display information for
	• ap-unadopted – Lists unadopted access-port
	• authorized-aps – Lists authorized APs detected by access-port scans
	• channel-power [11a|11b|11bg] – Lists the available channel and power levels for a radio
	• client [exclude-list|include-list] – Displays wireless client exclude and include lists
	• config – Displays wireless configuration parameters
	• country-code-list – Lists the supported country names and the corresponding ISO 3166 codes
	• default-ap – Displays default access-port information
	• fw [config] – Displays firewall information.
	  • config – Displays configurable firewall parameters
	• fwupdate-filelocation – Displays firewall update file location
	• fwupdate-filename – Displays firewall update file name
	• fwupdate-mode – Displays firmware upgrade modefwupdate-serveraddress – Displays SFTP server IP address
	• fwupdate-username – Displays login user name
	• hotspot <query> – Displays hotspot configuration
	  • query – Displays hotspot query string configuration
	• hotspot-config {<1-256>} – Displays the hotspot configuration for a WLAN of the index <1-256>
	• ignored-aps – Displays ignored APs seen by access-port scans

	• known {ap} – Displays known AP parameters
	  • ap [statistics] – Displays known AP statistics
	  • statistics {<1-1024>} – Displays one or more adaptive AP for known AP statistics of the index value <1-1024>
	• mac-auth-local {<1-1000>} – Lists all mac-auth-local entries
	  • <1-1000> – Displays the mac-auth-local entry specified by the <1-1000> value
	• mesh [statistics] – Displays mesh related parameters
	  • statistics {<1-32>} – Displays statistics for mesh of index <1-32>
	• mobile-unit [<1-8192> |<AA-BB-CC-DD-EE-FF>| association-history|association-stats|probe-history|radio|roaming| statistics|voice|wlan] – Displays details of associated mobile-units
	  • <1-8192> – The index of address of mobile units to display details for
	  • <AA-BB-CC-DD-EE-FF> – The MAC address of mobile units to display details for
	  • association-history – Displays mobile-unit history
	  • associations-stats – Displays statistics of associations and reassociations
	  • probe-history [<1-200> |config-list] – Displays mu probe-history
	  • <1-200> – index of mobile-unit to display probe logging
	  • config-list – Lists probe history MAC addresses
	  • radio <1-4096> – Displays mobile-units associated to this radio
	  • <1-4096> – The radio index to display mobile-units for
	  • roaming [database] – Displays mobile-unit inter-switch roaming
	  • database – Displays local mobile-unit roaming database
	  • statistics {<1-8192>|<AA-BB-CC-DD-EE-FF>|summary|voice}
	  • <1-8192> – Index of mobile-unit to display statistics for
	  • AA-BB-CC-DD-EE-FF – MAC address of the mobile-unit to display statistics for
	  • summary – Displays RF-stats summary for all currently associated mobile units
	  • voice [<1-8192>|<AA-BB-CC-DD-EE-FF>] – Displays mobile-unit voice statistics
	  • <1-8192> – Index of mobile-unit to display voice statistics for
	  • AA-BB-CC-DD-EE-FF – MAC address of the mobile-unit to display voice statistics for
	  • voice – Displays voice call details
	  • wlan [WLAN_RANGE] <1-256> – Displays mobile units associated with this wlan with an index value of <1-256>

wlan-acl [<1-256> |all	Displays WLAN ACL details • <1-256> – Displays ACLs attached to the specified WLAN ID • all – Displays ACLs attached to WLAN port

Usage Guidelines

Refer to *show on page 2-25* for details of show command.

Example

```
RFS7000(config)#show ?
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  audit-log-filters      Display audit log filter rules
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  fips-default-rules     FIPS Default Rules ID
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy-group       Display redundancy group parameters
  redundancy-history     Display state transition history of the switch.
  redundancy-members     Display redundancy group members in detail
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open connections
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  upgrade-status         Display last image upgrade status
  users                  Display information about currently logged in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl

RFS7000(config)#show


RFS7000(config)#show running-config
!
! configuration of RFS7000 version 1.1.0.0-36536X
!
version 1.0
!
!
aaa authentication login default local none
```

```
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!!
spanning-tree mst cisco-interoperability enable
spanning-tree mst config
 name My Name.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
wireless
 !
 wlan 1 enable
 wlan 1 ssid ajit-open
 aap local-bridging enable
 aap independent-vlan vlan 1
 aap config-apply def-delay 100
 aap config-apply mesh-delay 100
 radio add 1 00-A0-F8-BF-8A-4B 11bg ap300
 radio 1 rss enable
 radio add 2 00-A0-F8-BF-8A-4B 11a ap300
 radio 2 rss enable
 radio default-11a rss enable
 radio default-11bg rss enable
 radio default-11b rss enable
 radio 1 neighbor-smart-scan 1
 ids anomaly-detection bad-essid-frame enable
 service wireless map-radios 1
 service wireless legacy-load-balance
 enhanced-beacon-table enable
 enhanced-beacon-table max-ap 5
 enhanced-beacon-table scan-interval 30
 enhanced-beacon-table scan-time 500
 enhanced-beacon-table channel-set bg 1
 enhanced-probe-table enable
 enhanced-probe-table window-time 20
 enhanced-probe-table preferred 11-22-33-44-55-66
.....................................................................
.....................................................................
.....................................................................
.....................................................................
RFS7000(config)#
```

5.1.39 smtp-notification

Global Configuration Commands

Use this command to configure/modify the *Simple Mail Transfer Protocol* (SMTP) notification parameters.

Syntax

```
smtp-notification [authenticate|enable|password|port|prefix|recipient|
  sender|smtp-server-address|user]

smtp-notification authenticate enable
smtp-notification password [0 <PASSWORD>]
smtp-notification enable
smtp-notification port <1-65535>
smtp-notification prefix <WORD>
smtp-notification recipient <1-4> <LINE>
smtp-notification sender <LINE>
smtp-notification smtp-server-address <IP-ADDRESS>
smtp-notification user <USER-NAME>
```

Parameters

authenticate [enable]	Enables SMTP server authentication
enable	Enables SMTP trap notification
password [0 <PASSWORD>]	Configures SMTP authentication password • 0 <PASSWORD> – Configures unencrypted password. Specify a password up to 64 characters in length
port <1-65535>	Configures the SMTP server *Transmission Control Protocol* (TCP) port • <1-65535> – Specify the port to connect to the SMTP server between 1 - 65535.
prefix <WORD>	Configures the SMTP subject prefix • <WORD> – Specify the SMTP subject prefix (should not exceed 16 characters in length).
recipient <1-4>	Configures a maximum of 4 SMTP notification recipients • <1-4> <LINE> – Select the recipient index. • <LINE> – Specify the recipient address (should not exceed 128 characters in length).
sender <LINE>	Configures the SMTP sender address • <LINE> – Specify the sender address (should not exceed 128 characters in length).
smtp-server-address <IP-ADDRESS>	Configures the host to receive the SMTP notifications • <IP-ADDRESS> – Enter SMTP Server IP address/hostname (should not exceed 128 characters in length).
user <USER-NAME>	Configures the SMTP authentication user • <USER-NAME> – Enter the user name (should not exceed 64 characters in length)

Example

```
  RFS7000(config)#smtp-notification authenticate enable
  RFS7000(config)#

  RFS7000(config)#smtp-notification enable
  RFS7000(config)#

  RFS7000(config)#smtp-notification port 200
  RFS7000(config)#

  RFS7000(config)#smtp-notification user tester1

RFS7000(config)#

  RFS7000(config)#show smtp-notification
  ------------------------------------------------------------------------
  Global enable flag for Trap SMTP-Notification           Enabled
  ------------------------------------------------------------------------

  SMTP Server:
  SMTP Port:                      200
  SMTP Sender:
  SMTP Recipient 1:
  SMTP Recipient 2:
  SMTP Recipient 3:
  SMTP Recipient 4:
  SMTP Subject Prefix:
  SMTP Authentication:            Enabled
  SMTP Authentication User:       tester1
  SMTP Authentication Password:
  RFS7000(config)#
```

5.1.40 snmp-server

Global Configuration Commands

Use this parameter to configure/modify SNMP engine parameters.

Syntax

```
snmp-server [enable|engineid|host|location|manager|
  periodic-heartbeat-interval|sysname|user]

snmp-server enable traps {all|dhcp-server|diagnostics|miscellaneous|mobility|
nsm|radius-server|redundancy|snmp|wireless|wireless-statistics}

snmp-server engineid {netsnmp <HEX-String-EngineID>|text <TEXT-String-EngineID>}snmp-
server host [<IP-Address>] [v3] {<1-65535>}
snmp-server location <LINE>
snmp-server manager [v3]
snmp-server periodic-heartbeat-interval <10-1000>
snmp-server sysname <LINE>
snmp-server user [snmpmanager|snmpoperator|snmptrap] [v3] {auth|encrypted}
  (sha <password>)
```

Parameters

enable	Enables SNMP traps
engineid {netsnmp|text}	Configures the SNMP engine ID • netsnmp <WORD> – Optional. Sets the engine ID as a HEX string • text <WORD> – Optional. Sets the engine ID as a TEXT string
host <IP-ADDRESS>	Configures the SNMP Server host • <IP-ADDRESS> [v3] – Enter the host IP address in the A.B.C.D format. • v3 {<1-65535>} – Uses SNMP version 3 • <1-65535> – Optional. Configures the port ID to connect to the SNMP Server between 1 - 65535
location <LINE>	Configures the physical location of this node
manager [v3]	Enables version 3 SNMP manager
periodic-heartbeat-interval [<10-1000>]	Configures the periodic heartbeat interval between 10 - 1000 seconds. This is the interval after which a heartbeat trap is sent out if no other trap is sent by the switch. (default is 60 seconds)
sysname <LINE>	Configures the SNMP system name of the module
user [snmpmanager| snmpoperator|snmptrap]	Defines the user having access to the SNMP engine • snmpmanager – User is a manager • snmpoperator – User is an operator • snmptrap – User is a trap user

Example

```
RFS7000(config)#snmp-server enable traps all
RFS7000(config)#

RFS7000(config)#snmp-server periodic-heartbeat-interval 100
RFS7000(config)#
```

```
RFS7000(config)#snmp-server sysname SNMPEngine1
SNMPEngine1(config)#

SNMPEngine1(config)#show snmp-server
Location:
Contact:
SysName: SNMPEngine1

SNMP v3: enabled

SNMP host: num receivers = 0
SNMPEngine1(config)#
```

5.1.41 spanning-tree

Global Configuration Commands

Use this command to configure the spanning-tree commands.

Syntax

```
spanning-tree [mst|portfast]

spanning-tree mst [<0-15> (priority <0-61440>)|
  cisco-interoperability (enale|disable)|configuration|
  forward-time <4-30>|hello-time <1-10>|max-age <6-40>|max-hops <7-127>]

spanning-tree portfast [bpdufilter|bpduguard](default)
```

Parameters

spanning-tree (mst)	

mst
[<0-15> (priority <0-61440>)|
cisco-interoperability (enale|disable)|
configuration|
forward-time <4-30>|
hello-time <1-10>|
max-age <6-40>|
max-hops <7-127>]
	Enables the *Multiple Spanning Tree Protocol* (MSTP) on a bridge
	• <0-15> (priority <0-61440>) – Sets the bridge priority for an MST instance to the value specified. Use the `no` parameter with this command to restore the default bridge priority value.
	  • priority – Sets the bridge priority for the common instance
	  • <0-61440> – Sets the bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root)
	  The default value of the priority for each instance is 32768.
	• cisco-interoperability (enale|disable) – Enables/disables interoperability with CISCO's version of MSTP (incompatible with standard MSTP)
	  • enable – Enables CISCO Interoperability
	  • disable – Disables CISCO Interoperability
	• configuration – Multiple spanning tree configuration. This command moves to the *MST Config commands on page 13-1* instance.
	• forward-time <4-30> – Sets the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances. The default is 15 seconds.
	• hello-time <1-10> – Sets the hello-time. The hello-time is the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange *Bridge Protocol Data Units* (BPDUs). A very low value leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances. The default is 2 seconds.

Usage Guidelines

	• max-age <6-40> – Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value must be greater than twice the value of the hello time plus one, but less than twice the value of the forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the max-age. Use this command to set the max-age for a bridge. This value is used by all instances. The default bridge max-age is 20 seconds. • max-hops <7-127> – Specifies the maximum allowed hops for a BPDU in an MST region. This parameter is used by all MST instances. To restore the default value, use the no parameter with this command. The default max-hops in a MST region is 20.
spanning-tree (portfast)	
portfast [bpdufilter|bpduguard](default)	Enables the portfast feature on a bridge. It has the following options: • bpdufilter (default) – Use the bpdu-filter command to set the portfast BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFast enabled ports do not transmit or receive BPDUs. • bpduguard (default) – Use the bpdu-guard command to enable the BPDU Guard feature on a bridge. Use the no parameter with this command to disable BPDU Guard. When the BPDU Guard is set for a bridge, all portfast-enabled ports that have the bpdu guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. The port can be brought back up manually (using the no shutdown command), or by configuring a errdisable timeout to enable the port after the specified interval.

The `mst > configuration` command moves you to the *MST Config commands on page 13-1* instance.

If a bridge does not hear BPDUs from the root bridge within the specified interval defined in the max-age (seconds) parameter, assume the network has changed and recompute the spanning-tree topology.

Example

```
RFS7000(config)#spanning-tree portfast bpduguard default
RFS7000(config)#
```

5.1.42 timezone

Global Configuration Commands

Use this command to configure switch timezone settings.

Syntax

```
timezone
```

Parameters

TIMEZONE	Press <tab> to navigate the list of files. This action displays a list of files containing timezone information.

Example

```
RFS7000(config)#timezone
Africa/     America/    Asia/       Atlantic/   Australia/  Etc/        Europe/
Pacific/
RFS7000(config)#timezone

RFS7000(config)#timezone America/
America/Anchorage     America/Bogota        America/Buenos_Aires  America/Caracas
America/Chicago
America/Costa_Rica    America/Denver        America/Los_Angeles   America/Mexico_City
America/Montreal
America/New_York      America/Phoenix       America/Santiago      America/Sao_Paulo
America/St_Johns
America/Tegucigalpa   America/Thule         America/Winnipeg      America/Indianapolis

RFS7000(config)#timezone America/Chicago
RFS7000(config)#
```

5.1.43 traffic-shape

Global Configuration Commands

Use this command to configure traffic shaping, also know as packet shaping, parameters. Enabling traffic shaping regulates network data transfer and ensures a certain level of network performance. The traffic-shape command allows you to delay the flow of packets with low priority.

Syntax

```
traffic-shape [class|priority-map]

traffic-shape class <1-4> [max-buffers|max-latency|rate]
traffic-shape class <1-4> max-buffers (<1-2000>) {red-level (<1-2000>)|
  red-percent (<1-100>)}traffic-shape class <1-4> max-latency (<1-1000000>) [msec|usec]
traffic-shape class <1-4> rate <1-250000000> {Kbps|Mbps|bps}

traffic-shape priority-map (<0-7>)
```

Example

class <1-4> [max-buffers| max-latency|rate]	Configures traffic shaping packet class. A maximum of four traffic classes can be configured. Select the class index between 1 - 4 and define the following parameters: • max-buffers <1-2000> – Defines maximum queue lengths in packets between 1 - 2000 • max-latency <1-1000000> – Defines the maximum packet delay in queue between 1 - 1000000 • rate <1-250000000> – Defines the traffic rates in Kbps/Mbps/Bps The following priority queues are common to the 'max-buffers' and max-latency' keywords: • Priority 0 (background) queue • Priority 1 (background) queue • Priority 2 (default) queue • Priority 3 queue • Priority 4 queue • Priority 5 queue • Priority 6 queue • Priority 7 queue
priority-map <0-7>	Configures the 802.1p to priority queue map

```
RFS7000(config)#traffic-shape priority-map 1 2 3 4 5 6 7 7
RFS7000(config)#

RFS7000(config)#show traffic-shape priority-map
 802.1p | Shaping priority
     0  |  1
     1  |  2
     2  |  3
     3  |  4
     4  |  5
     5  |  6
     6  |  7
     7  |  7
RFS7000(config)#
```

5.1.44 username

Global Configuration Commands

Use this CLI command to establish the user name authentication.

Syntax

```
username <USER-NAME> {access|password|privilege}
username <USER-NAME> access [web|console|ssh]
username <USER-NAME password [0 <WORD>|1 <WORD>|<WORD>]
username <USER-NAME> privilege [crypto-officer|monitor|superuser|sysadmin|webadmin]
```

Parameters

<USER-NAME>	Enter a name to authenticate the switch. The username must be between 1 - 28 characters.
access	Optional. Sets the user access mode • web – Only allowed from applet (webUI) • console – Only allowed from console • ssh – Only allowed from ssh
password	Optional. Specifies the user password • 0 <WORD> – Password is specified UNENCRYPTED • 1 <WORD>– Password is encrypted with SHA1 algorithm • <WORD> – User defined password (must be a plaintext passsword of length between 8 - 32 characters)
privilege	Optional. Sets user access privileges • crypto-officer – Assigns cryptographic configurations and Network (wired/ wireless) admin access • monitor – Monitor (read-only) access • superuser – Superuser (root) access • sysadmin – System (general system configuration) admin access • webadmin – Web auth (hotspot) user admin access

Example

```
RFS7000(config)#username george privilege crypto-officer
RFS7000(config)#

RFS7000(config)#username john access console
RFS7000(config)#
```

5.1.45 virtual-ip

Global Configuration Commands

Displays virtual IP configuration for the switch.

Syntax

```
virtual-ip [<A.B.C.D/M>|advt-timeout|enable|garp-timeout|learning-timeout|priority|vmac]

virtual-ip <A.B.C.D/M> [vlan <1-4094>]
virtual-ip advt-timeout <1-5>
virtual-ip enable
virtual-ip garp-timeout <30-600>
virtual-ip learning-timeout <2-5>
virtual-ip priority [<1-256>|auto]
virtual-ip vmac <AA-BB-CC-DD-EE-FF>
```

Parameters

<A.B.C.D/M> [vlan <1-4094>]	Configures switch's virtual IP in the A.B.C.D/M format • vlan <1-4094> – Configures the VLAN interface for the virtual IP • <1-4094> – Select the VLAN interface index between 1 - 4094.
advt-timeout <1-5>	Configures the advertisement timeout in seconds • <1-5> – Specify the timeout period between 1 - 5 seconds.
enable	Enables the IP redundancy protocol
garp-timeout <30-600>	Configures the *gratituous ARP* (GARP) timeout in seconds • <30-600> – Specify the timeout period between 30 - 600 seconds.
learning-timeout <2-5>	Configures the learning timeout in seconds • <2-5> – Specify the timeout period between 2 -5 seconds.
priority [<1-256>|auto]	Configures the switch priority • <1-256> – Allows you to manually configure the switch priority between 1 - 256 • auto – Configures automatic priority selection mode
vmac <AA-BB-CC-DD-EE-FF>	Configures the virtual MAC used by the master • <AA-BB-CC-DD-EE-FF> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format. (allowed VMACs are: from 00:15:70:88:8a:90 to 00:15:70:88:8b:8f)

Example

```
RFS7000(config)#virtual-ip 1.2.3.4/24 vlan 11
RFS7000(config)#

RFS7000(config)#show virtual-ip config
Virtual-IP Status           : Disabled
Cluster Redundancy Status   : Disabled
Priority Selection Mode     : Automatic
Learning Timeout(sec)       : 2
Advertisement Timeout(sec)  : 1
Gratuitous ARP Timeout(sec) : 30
Virtual-IP Server Port      : 51525
Switch IP                   : 0.0.0.0
Reserved VMAC Address Range : 00-15-70-88-8A-90 to 00-15-70-88-8B-8F
Configured Virtual MAC      : Not Configured
DHCP Server status          : Not Running on this Switch
+-------------------------------------------------+
| Vlan |  Priority  |    SwitchID   |  Virtual IP   |
---------------------------------------------------+
|   11 | 0          |0.0.0.0        |1.2.3.4        |
+-------------------------------------------------

RFS7000(config)#
```

5.1.46 vpn

Global Configuration Commands

Use this command to configure *Virtual Private Network* (VPN).

Syntax

```
vpn authentication-method [local|radius]
```

Parameters

authentication-method	Selects the authentication scheme
local	Used for user based authentication
radius	Used for RADIUS server authentication

Usage Guidelines

VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. VPN uses "tunneling" to encrypt all information at the IP level.

Example

```
RFS7000(config)#vpn authentication-method local
RFS7000(config)#
```

5.1.47 wireless

Global Configuration Commands

Use this command to configure switch wireless parameters. This command leads moves to the `config-wireless` instance. For additional information, see *Wireless Configuration Commands on page 20-1*.

Syntax

```
wireless
```

Parameters

None

Usage Guidelines

The wireless command is used to enter the config-wireless instance. The prompt changes from the regular `RFS7000(config)#` to `RFS7000(config-wireless)#.`

Example

```
RFS7000(config)#wireless
RFS7000(config-wireless)#
```

5.1.48 wlan-acl

Global Configuration Commands

Use this command to apply an ACL on a WLAN index.

Syntax

```
wlan-acl <1-256> [<1-99>|<100-199>|<1300-1999>|<2000-2699>|<WORD>] [in|out]
```

Parameters

<1-256> [<1-99>|<100-199>| <1300-1999>| <2000-2699>|<WORD>]	Applies an ACL on the WLAN specified by the <1-256> parameter. Specify the access control list to apply, using one of the following options: • <1-99> – IP standard access list • <100-199> – IP extended access list • <1300-1999> – IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <WORD> – The access list name

Usage Guidelines

Every WLAN created is mapped to an index. When an ACL is applied on a WLAN index it becomes a WLAN ACL. The following ACLs can be applied on a WLAN:

- IP Standard ACL
- IP Extended ACL
- MAC Extended ACL

When a packet is sent from a client to a WLAN index of an access port, it becomes an inbound traffic to the wireless LAN.

When a packet goes out of a access port, it becomes a outbound traffic to the wireless LAN index. Apply an ACL to a WLAN index in the outbound direction to filter traffic from both wired and wireless interfaces.

`wlan-acl` can be attached both in the inbound and outbound directions.

NOTE Most of the Wireless LAN related configuration are performed using the *Wireless Configuration Commands on page 1*.

Use `wlan-acl` (in the global configuration mode) to apply an ACL on a wireless LAN index .

The last ACE in the access list is an implict deny statement. Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

Example

The example below applies an ACL to WLAN index 200 in an inbound direction from the global config mode.

```
RFS7000(config)#wlan-acl 200 150 in
RFS7000(config)#
```

NOTE A MAC access list entry to allow `arp` is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The example below applies an ACL to WLAN index 200 in an outbound direction from the global config mode.

```
RFS7000(config)#wlan-acl 200 150 out
RFS7000(config)#
```

5.1.49 zeroize

Global Configuration Commands

Use this command for zeroization of critical security parameters.

NOTE In RFS7000, key zeroisation function zeroises all Cryptographic Keys and Critical Security Parameters (CSP) by overwriting the storage area three times with an alternating pattern (i.e, three different patterns).

Syntax

```
zeroize [keys]
```

Parameters

keys	All security related keys

Example

```
RFS7000(config)#zeroize keys
Do you want to continue [y/n]?
RFS7000(config)#
```

6

Crypto - isakmp Instance

The `(config-crypto-isakmp)` instance is used to configure *Internet Security and Key Management Protocol* (ISAKMP) policy.

To instantiate the `(config-crypto-isakmp)` instance, use the following command:

```
RFS7000(config)#crypto isakmp policy <1-10000>
RFS7000(config-crypto-isakmp)#
```

6.1 Crypto ISAKMP Config Commands

Table 6.1 summarizes the **`crypto-isakmp`** commands within the RFS7000 switch command line interface.

Table 6.1 Crypto ISAKMP Command Summary

Command	Description	Ref.
authentication	Sets the authentication method for protection suite	*page 6-2*
clrscr	Clears the display screen	*page 6-3*
encryption	Sets encryption algorithm for the protection suite	*page 6-4*
end	Ends current mode and change to EXEC mode	*page 6-5*
exit	Ends current mode and moves to previous mode	*page 6-6*
hash	Sets hash algorithm for protection suite	*page 6-7*
help	Displays the interactive help system	*page 6-8*
lifetime	Sets the lifetime for ISAKMP security associations	*page 6-9*
no	Negates a command or set its defaults	*page 6-10*
service	Displays service commands	*page 6-11*
show	Shows running system information	*page 6-11*

6.1.1 authentication

Crypto ISAKMP Config Commands

Use this command to set **pre-shared** key as the authentication method for this protection suite.

Syntax

```
authentication [pre-share]
```

Parameters

pre-share	Sets pre shared key as the authentication method

Example

```
RFS7000(config-crypto-isakmp)#authentication pre-share
RFS7000(config-crypto-isakmp)#
RFS7000(config-crypto-isakmp)#show crypto isakmp policy 1
Protection suite sequence number 1
encryption algorithm: AES - Advanced Encryption Standard (256 - bit keys )
 hash algorithm: Secure Hash Standard
 authentication method: preshared key
 Diffie-Hellman group: #14 (2048 bit)
 lifetime:  86400 seconds, no volume limit
RFS7000(config-crypto-isakmp)#
```

6.1.2 clrscr

Crypto ISAKMP Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-crypto-isakmp)#clr
RFS7000(config-crypto-isakmp)#
```

6.1.3 encryption

Crypto ISAKMP Config Commands

Use this command to configure the data encryption algorithm used with this protection suite.

Syntax

```
encryption [aes|aes-192|aes-256]
```

Parameters

aes	Configures the *Advanced Encryption Standard* (AES) (128 bit key)
aes-192	Configures 192 bit AES key
aes-256	Configures 256 bit AES key

Example

```
RFS7000(config-crypto-isakmp)#encryption aes-256
RFS7000(config-crypto-isakmp)#

RFS7000(config-crypto-isakmp)#show crypto isakmp policy 1
Protection suite sequence number 1
 encryption algorithm: AES - Advanced Encryption Standard (256 - bit keys )
 hash algorithm: Secure Hash Standard
 authentication method: preshared key
 Diffie-Hellman group: #14 (2048 bit)
 lifetime:  86400 seconds, no volume limit
RFS7000(config-crypto-isakmp)#
```

6.1.4 end

Crypto ISAKMP Config Commands

Use this command to end and exit the `(config-crypto-isakmp)` mode and move to the PRIV EXEC mode. The prompt now changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-crypto-isakmp)#end
RFS7000#
```

6.1.5 exit

Crypto ISAKMP Config Commands

Use this command to exit the `(config-crypto-isakmp)` mode and move to the previous GLOBAL CONFIG mode. The prompt now changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-crypto-isakmp)#exit
RFS7000(config)#
```

6.1.6 hash

Crypto ISAKMP Config Commands

Use this command to configure the hash algorithm used to authenticate data transmitted over the *Internet Key Exchange* (IKE) *Security Association* (SA).

Syntax

```
hash [sha]
```

Parameters

sha	Sets *Security Hash Standard* (SHA) hash algorithm for this protection suite

Example

```
RFS7000(config-crypto-isakmp)#hash sha
RFS7000(config-crypto-isakmp)#

Protection suite sequence number 1
 encryption algorithm: AES - Advanced Encryption Standard (256 - bit keys )
 hash algorithm: Secure Hash Standard
 authentication method: preshared key
 Diffie-Hellman group: #14 (2048 bit)
 lifetime:  86400 seconds, no volume limit
SNMPEngine1(config-crypto-isakmp)#
```

6.1.7 help

Crypto ISAKMP Config Commands

Use this command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-crypto-isakmp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-crypto-isakmp)#
```

6.1.8 lifetime

Crypto ISAKMP Config Commands

Use this command to specify how long an IKE SA is valid before expiring.

Syntax

```
lifetime <seconds>
```

Parameters

<seconds>	Specifies how many seconds an IKE SA lasts before it expires. This is an IPsec Phase 1 SA lifetime. Time stamp can be configured between 180 - 86400 seconds (default is 86400 seconds).

Example

```
RFS7000(config-crypto-isakmp)#lifetime 5200
RFS7000(config-crypto-isakmp)#

RFS7000(config-crypto-isakmp)#show crypto isakmp policy 1
Protection suite sequence number 1
 encryption algorithm: AES - Advanced Encryption Standard (256 - bit keys )
 hash algorithm: Secure Hash Standard
 authentication method: preshared key
 Diffie-Hellman group: #14 (2048 bit)
 lifetime:  5200 seconds, no volume limit
RFS7000(config-crypto-isakmp)#
```

6.1.9 no

Crypto ISAKMP Config Commands

Use the `no` command in the `(config-crypto-isakmp)` mode to negate or reset values to default settings.

Syntax

```
no [authentication|encryption|hash|lifetime]
RFS7000(config-crypto-isakmp)#no lifetime
```

no authentication	Resets the authentication method to default (preshared key)
no encryption	Resets the encryption algorithm to default (aes)
no hash	Resets the hash algorithm for the protection suite to default (SHA)
no lifetime	Resets the ISAKMP SA lifetime to default (86400 seconds)

```
RFS7000(config-crypto-isakmp)#
```

6.1.10 service

Crypto ISAKMP Config Commands

Use this command to view the `(config-crypto-isakmp)` instance CLI configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Displays CLI tree of current mode

Example

```
RFS7000(config-crypto-isakmp)#service show cli
Crypto Isakmp Config mode:
+-authentication
  +-pre-share [authentication ( pre-share )]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-encryption
  +-aes [encryption ( aes | aes-192 | aes-256 )]
  +-aes-192 [encryption ( aes | aes-192 | aes-256 )]
  +-aes-256 [encryption ( aes | aes-192 | aes-256 )]
+-end [end]
+-exit [exit]
+-group
  +-2 [group (2|5)]
  +-5 [group (2|5)]
+-hash
  +-sha [hash (sha)]
.....................................................................
.....................................................................
RFS7000(config-crypto-isakmp)#
```

6.1.11 show

Crypto ISAKMP Config Commands

Use this CLI command to view the current system information that is running on the RFS7000 switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which the information can be viewed using show command.

Example

```
RFS7000(config-crypto-isakmp)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
```

```
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-crypto-isakmp)#
```

7

Crypto - group Instance

The (config-crypto-group) instance configures the default group properties of the ISAKMP client.

To instantiate the `config-crypto-group` instance, use the following command:

```
RFS7000(config)#crypto isakmp client configuration group default
RFS7000(config-crypto-group)#
```

7.1 Crypto Group Config Commands

Table 7.1 summarizes the **`config-crypto-group`** commands within the RFS7000 switch command line interface.

Table 7.1 Crypto Group Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 7-2*
dns	Configures *Domain Name Server* (DNS)	*page 7-3*
end	Ends the current mode and moves to EXEC mode	*page 7-4*
exit	Ends the current mode and moves to previous mode	*page 7-5*
help	Description of the interactive help system	*page 7-6*
service	Displays service commands	*page 7-7*
show	Shows running system information	*page 7-8*
wins	Configures *Windows Name Server* (WINS)	*page 7-10*

7.1.1 clrscr

Crypto Group Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-crypto-group)#clr
RFS7000(config-crypto-group)#
```

7.1.2 dns

Crypto Group Config Commands

Use this command to specify the DNS Server address(es) to assign to a client.

Syntax

```
dns <A.B.C.D>
```

Parameters

<A.B.C.D>	Specify the first DNS server's address in the A.B.C.D format.

Example

```
RFS7000(config-crypto-group)#dns-server 172.1.17.1
RFS7000(config-crypto-group)#
```

7.1.3 end

Crypto Group Config Commands

Use this command to end and exit from the `(config-crypto-group)` mode and move to the PRIV EXEC mode.The prompt now changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-crypto-group)#end
RFS7000#
```

7.1.4 exit

Crypto Group Config Commands

Use this command to end the `(config-crypto-group)` mode and move to the previous GLOBAL CONFIG mode. The prompt now changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-crypto-group)#exit
RFS7000(config)#
```

7.1.5 help

Crypto Group Config Commands

Use this command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-crypto-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-crypto-group)#
```

7.1.6 service

Crypto Group Config Commands

Use this command to invoke the service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Displays CLI tree of current mode

Example

```
RFS7000(config-crypto-group)#service show cli
Crypto Client Config mode:
+-clrscr [clrscr]
+-dns
  +-A.B.C.D [dns A.B.C.D]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
.....................................................................
.....................................................................
RFS7000(config-crypto-group)#
```

7.1.7 show

Crypto Group Config Commands

Use this command to view the current system information that is running on the RFS7000 switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which the information can be viewed using the `show <cmd>` command

Example

```
RFS7000(config-crypto-group)#show ?
  aap-wlan-acl           wlan based acl
   aap-wlan-acl-stats    IP filtering wlan based statistics
   access-banner         Display Access Banner
   access-list           Internet Protocol (IP)
   aclstats              Show ACL Statistics information
   alarm-log             Display all alarms currently in the system
   audit-log-filters     Display audit log filter rules
   autoinstall           autoinstall configuration
   boot                  Display boot configuration.
   clock                 Display system clock
   commands              Show command lists
   crypto                encryption module
   crypto-error-log      Display Crypto Error Log
   crypto-log            Display Crypto Log
   debugging             Debugging information outputs
   dhcp                  DHCP Server Configuration
   environment           show environmental information
   file                  Display filesystem information
   firewall              Wireless firewall
   history               Display the session command history
   interfaces            Interface status
   ip                    Internet Protocol (IP)
   ldap                  LDAP server
   licenses              Show any installed licenses
   logging               Show logging configuration and buffer
   mac                   Internet Protocol (IP)
   mac-address-table     Display MAC address table
   mac-name              Displays the configured MAC Names
   management            Display L3 Managment Interface name
   mobility              Display Mobility parameters
   ntp                   Network time protocol
   password-encryption   password encryption
   port                  Physical/Aggregate port interface
   port-channel          Portchannel commands
   privilege             Show current privilege level
   protocol-list         List of protocols
   radius                RADIUS configuration commands
   redundancy            Configure redundancy group parameters
   role                  Configure role parameters
   rtls                  Real Time Locating System commands
   running-config        Current Operating configuration
   securitymgr           Securitymgr parameters
   service-list          List of services
   sessions              Display current active open connections
   smtp-notification     Display SNMP engine parameters
   snmp                  Display SNMP engine parameters
   snmp-server           Display SNMP engine parameters
   spanning-tree         Display spanning tree information
   startup-config        Contents of startup configuration
   static-channel-group  static channel group membership
   terminal              Display terminal configuration parameters
   timezone              Display timezone
   traffic-shape         Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-crypto-group)#
```

7.1.8 wins

Crypto Group Config Commands

Use this command to specify the *Windows Internet Naming Service* (WINS) name servers to assign to a client.

Syntax

```
wins <A.B.C.D>
```

Parameters

<A.B.C.D>	Specify the first WINS server's IP address in the A.B.C.D format.

Example

```
RFS7000(config-crypto-group)#wins 128.2.11.1
RFS7000(config-crypto-group)#
```

8

Crypto - peer Instance

The `(config-crypto-peer)` instance is used to configure ISAKMP peers.

To instantiate the `(config-crypto-peer)` instance, use the following command:

```
RFS7000(config)#crypto isakmp peer hostname [<PEER-IP-ADDRESS>|<PEER-DN>|<PEER-
  HOSTNAME>]
RFS7000(config)#crypto isakmp peer hostname <WORD>
RFS7000(config-crypto-peer)#
```

8.1 Crypto Peer Config Commands

Table 8.1 summarizes the **`config-crypto-peer`** commands within the RFS7000 switch command line interface.

Table 8.1 Crypto Peer Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 8-2*
end	Ends the current mode and moves to EXEC mode	*page 8-3*
exit	Ends the current mode and moves to the previous mode	*page 8-4*
help	Displays the interactive help system	*page 8-5*
no	Negates a command or sets its defaults	*page 8-6*
service	Displays service commands	*page 8-7*
set	Sets the configuration	*page 8-8*
show	Shows running system information	*page 8-9*

8.1.1 clrscr

Crypto Peer Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-crypto-peer)#clr
RFS7000(config-crypto-peer)
```

8.1.2 end

Crypto Peer Config Commands

Use this command to end and exit the `(config-crypto-peer)` mode and move to the PRIV EXEC mode.The prompt now changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-crypto-peer)#end
RFS7000#
```

8.1.3 exit

Crypto Peer Config Commands

Use this command to end the `(config-crypto-peer)` mode and move to the previous mode (GLOBAL-CONFIG). The prompt now changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-crypto-peer)#exit
RFS7000(config)#
```

8.1.4 help

Crypto Peer Config Commands

Use this command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFS7000(config-crypto-peer)#
```

8.1.5 no

Crypto Peer Config Commands

Use this command to negate a command or set its defaults.

Syntax

```
no <previous command used>
```

Parameters

Use the commands that you have configured under this instance.

Example

```
RFS7000(config-crypto-peer)#no aggrerssive-mode
RFS7000(config-crypto-peer)#
```

8.1.6 service

Crypto Peer Config Commands

Use this command to invoke the service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Displays CLI tree of current mode

Example

```
RFS7000(config-crypto-peer)#service show cli
Crypto Peer Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-crypto-peer)#
```

8.1.7 set

Crypto Peer Config Commands

Use this command to configure the aggressive-mode attributes for this crypto peer.

Syntax

```
set aggressive-mode password [0 <WORD>|2 <WORD>|<WORD>]
```

Parameters

aggressive-mode	Configures aggressive mode attributes
password [0 <WORD>| 2 <WORD>|<WORD>]	Configures tunnel password attributes • 0 <WORD> – Password is specified UNENCRYPTED. • 2 <WORD> – Password is specified encrypted with password-encryption secret. • <WORD> – Specify the password (minimum 8 characters in length).

Example

```
RFS7000(config-crypto-peer)#set aggressive-mode password CheckMeIn
RFS7000(config-crypto-peer)#
```

8.1.8 show

Crypto Peer Config Commands

Use this command to view the current system information that is running on the RFS7000 switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
RFS7000(config-crypto-peer)#show ?
aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-crypto-peer)#
```

9

Crypto - ipsec Instance

Use the `crypto ipsec transform-set <transform set name>` command to define a transform configuration for securing data using esp-aes or esp-sha-hmac or other cipher modes.

To instantiate the `(config-crypto-ipsec)` instance, use the following command:

```
RFS7000(config)#crypto ipsec transform-set <TRANSFORM-SET-NAME> <ENCRYPTION-TYPE>
  {esp-sha-hmac}
RFS7000(config-crypto-ipsec)#
```

The transform-set is assigned to a crypto map using the map's `set transform-set` command. For more details on the crypto-map transform-set command, see *set on page 10-9*.

9.1 Crypto IPSec Config Commands

Table 9.1 summarizes the **`config-crypto-ipsec`** commands within the RFS7000 Switch command line interface.

Table 9.1 Crypto IPSec Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 9-2*
end	Ends the current mode and moves to the EXEC mode	*page 9-3*
exit	Ends the current mode and moves to the previous mode	*page 9-4*
help	Displays the interactive help system	*page 9-5*
mode	Configures IPSec encapsulation (transport/tunnel) mode	page 9-6
no	Negates a command or sets its defaults	*page 9-7*
service	Displays service commands	*page 9-8*
show	Shows running system information	*page 9-9*

9.1.1 clrscr

Crypto IPSec Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-crypto-ipsec)#clr
RFS7000(config-crypto-ipsec)
```

9.1.2 end

Crypto IPSec Config Commands

Use this command to end and exit the `config-crypto-ipsec` mode and move to the PRIV EXEC mode.The prompt now changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-crypto-ipsec)#end
RFS7000#
```

9.1.3 exit

Crypto IPSec Config Commands

Use this command to end the `config-crypto-ipsec` mode and move to the previousGLOBAL CONFIG mode. The prompt now changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000 (config-crypto-ipsec)#exit
RFS7000(config)#
```

9.1.4 help

Crypto IPSec Config Commands

Use this command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-crypto-ipsec)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFS7000(config-crypto-ipsec)#
```

9.1.5 mode

Crypto IPSec Config Commands

Use this command to configure the IPSec encapsulation (trasnport/tunnel) mode.

Syntax

```
mode [transport|tunnel]
```

Parameters

transport	Configures the transport (payload encapsulation) mode
tunnel	Configures the tunnel (datagram encapsulation) mode (default)

Example

```
RFS7000(config-crypto-ipsec)#mode transport
RFS7000(config-crypto-ipsec)#

RFS7000(config-crypto-ipsec)#show crypto ipsec transformset TranSet1
Transform set TranSet1: {esp-aes esp-sha-hmac}
         will negotiate = { transport,  },
RFS7000(config-crypto-ipsec)#
```

9.1.6 no

Crypto IPSec Config Commands

Use the `no` command in the `config-crypto-ipsec` mode to negate the `mode` command and revert to the default tunnel (datagram encapsulation) mode.

Syntax

```
no [mode]
```

Parameters

Use the commands that you have configured under this instance.

Example

```
RFS7000(config-crypto-ipsec)#no mode
RFS7000(config-crypto-ipsec)#

RFS7000(config-crypto-ipsec)#show crypto ipsec transformset TranSet1
Transform set TranSet1: { esp-aes esp-sha-hmac}
         will negotiate = { tunnel,  },
RFS7000(config-crypto-ipsec)#
```

9.1.7 service

Crypto IPSec Config Commands

Use this command to invoke the service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows CLI tree of current mode

Example

```
RFS7000(config-crypto-ipsec)#service show cli
Crypto Ipsec Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
 -- MORE --, next page: Space, next line: Enter, quit: Control-C....

RFS7000(config-crypto-ipsec)#
```

9.1.8 show

Crypto IPSec Config Commands

Use this command to view the current system information that is running on the RFS7000 switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command.

Example

```
RFS7000 (config-crypto-ipsec)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-crypto-ipsec)#
```

10

Crypto - map Instance

Use the `crypto map <crypto map name>` command to define a crypto map.

The `config-crypto-map` CLI commands define a *Certificate Authority* (CA) trustpoint. This is a separate instance by itself but belongs to the `crypto pki trustpoint` mode under the `config` instance.

To instantiate the `(config-crypto-map)` instance, use the following command:

```
RFS7000(config)#crypto map <MAP-NAME> <MAP-SEQUENCE> [ipsec-isakmp|ipsec-manual]
{dynamic}
RFS7000(config-crypto-map)#
```

10.1 Crypto Map Config Commands

Table 10.1 summarizes the **`config-crypto-map`** commands within the RFS7000 Switch command line interface.

Table 10.1 Crypto Map Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 10-2*
end	Ends the current mode and moves to the EXEC mode	*page 10-3*
exit	Ends the current mode and moves to previous mode	*page 10-4*
help	Displays the interactive help system	*page 10-5*
match	Matches values	*page 10-6*
no	Negates a command or sets its defaults	*page 10-7*
service	Displays service commands	*page 10-8*
set	Sets values for encryption/decryption	*page 10-9*
show	Shows running system information	*page 10-12*

10.1.1 clrscr

Crypto Map Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-crypto-map)#clr
RFS7000(config-crypto-map)
```

10.1.2 end

Crypto Map Config Commands

Use this command to end and exit the `config-crypto-map` mode and move to the PRIV EXEC mode.The prompt now changes to `RFS7000#`.

Syntax

```
end
```

Parameters

ExampleNone

```
RFS7000(config-crypto-map)#end
RFS7000#.
```

10.1.3 exit

Crypto Map Config Commands

Use this command to end the `config-crypto-map` mode and move to the previous GLOBAL CONFIG mode. The prompt now changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-crypto-map)#exit
RFS7000(config)#
```

10.1.4 help

Crypto Map Config Commands

Use this command to access the systems interactive help system

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-crypto-map)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFS7000(config-crypto-map)#
```

10.1.5 match

Crypto Map Config Commands

Use this command to assign an IP access list to a crypto map definition. The access list designates the IP packets encrypted by this crypto map.

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: ipsec-manual and ipsec-isakmp. Each entry is given an index used to sort the ordered list.

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable SA exists, that is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists, and the crypto map entry is “respond only”, the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

Syntax

```
match [address] <ACL-NAME/ID>
```

Parameters

address <ACL-NAME/ID>	Enter the ACL name/ID to assign to this crypto map.

Usage Guidelines

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An *access control list* (ACL) is assigned to the crypto map using the match address command. If no ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the OS product. The source information must be the local OS product and the destination must be the peer.

Only extended access-lists can be used in crypto maps.

Example

The following example configures an ACL (called TestList) and assigns it to a crypto map (called TestMap):

```
RFS7000(config)#ip access-list extended TestList
Configuring New Extended ACL "TestList"
(config-ext-nacl)#exit

RFS7000(config)#crypto map TestMap 220 ipsec-isakmp dynamic
RFS7000(config-crypto-map)#

RFS7000(config-crypto-map)#match address TestList
RFS7000(config-crypto-map)#
```

10.1.6 no

Crypto Map Config Commands

Use the `no` command in the `config-crypto-map` mode to negate or revert the `match` and `set` commands.

Syntax

```
no [match|set]
```

Parameters

match	Negates the `match` command. Removes the access list associated with this crypto map using the `match` command
set	Negates values set for encryption/decryption

Example

```
RFS7000(config-crypto-map)#no match address TestList
RFS7000(config-crypto-map)#
```

10.1.7 service

Crypto Map Config Commands

Use this command to invoke the service commands to troubleshoot or debug the `(config-crypto-map)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Displays CLI tree of current mode

Example

```
RFS7000(config-crypto-map)#service show cli
Crypto Map Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
 -- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-crypto-map)#
```

10.1.8 set

Crypto Map Config Commands

Use this command to set the various set parameters of the peer device.

Syntax

```
set [localid|mode|peer|pfs|remote-type|security-association|session-key|transform-set]
set localid [dn|hostname] <WORD>
set mode [main]
set peer [<A.B.C.D>|<WORD>]
set pfs
set remote-type [ipsec-12tp|xauth]
set security-association [level (perhost)|lifetime (kilobytes <value>|seconds <value>)]
set session-key [inbound|outbound] [ah|esp]
set session-key [inbound|outbound] ah <SPI> <WORD>
set session-key [inbound|outbound] esp <SPI> cipher <WORD> authenticator <WORD>
set transform-set <WORD>
```

Parameters

localid [dn|hostname]	Sets this crypto map's local identity using one of the following options: • dn <WORD> – Specifies the distinguished name • hostname <WORD> – Specifies the hostname • <WORD> – The distinguished name/hostname
mode [main]	Sets this crypto map's tunnel mode. • main – Initiates main mode.
peer [<A.B.C.D>|<WORD>]	Sets the peer device's IP address. This can be set for multiple remote peers. Remote peer can be identified either by IP addresses or hostnames. **Note:** For manual mode, only one remote peer can be added to a crypto map. • <A.B.C.D> – Enter the peer device's IP address. If this is not configured, it implies respond to any peer. • <WORD> – Enter the peer device's hostname.
pfs	Sets the *perfect forward secrecy* (pfs) (if any) required during IPSec negotiation of security associations for this crypto map. Use the `no` form of this command to require no PFS. • group 14 – IPSec is required to use Diffie-Hellman Group 14 (2048-bit modulus) exchange during IPSec SA key generation
remote-type [ipsec-12tp|xauth]	Sets the remote VPN client type • ipsec-l2tp – Specifies remote VPN client as using IPSec/L2TP • xauth – Specifies remote VPN client as using XAUTH with mode config

security-association [level|lifetime]	Defines the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map
	• level [perhost] – Specifies the security association granularity to the host level. This option requests for separate IPSec SAs for each source/ destination host pair.
	• lifetime [kilobytes|seconds] – Specifies the security association lifetime. This is an IPsec Phase 2 SA lifetime. This option overrides the global lifetime value used when negotiating IPSec SAs.
	  • kilobyte – Configures volume-based key duration. (minimum is 500KB and maximum is 204800KB). The default value is 204800KB.
	  • seconds – Configures time-based key duration. (minimum is 90 seconds and maximum is 28800 seconds). The default value is 3600seconds.

session-key [inbound|outbound]	Defines the encryption and authentication keys for this crypto map
	• inbound – Defines encryption keys for inbound traffic
	• outbound – Defines encryption keys for outbound traffic
	Use following keywords to define encryption keys for inbound/outbound traffic:
	• ah <256-4294967295> <WORD> – Configures an *Authentication Header* (AH) key for security associations. Specify the key's *Security Parameter Index* (SPI) between 256 - 4294967295.
	  • <WORD> – Specify the security association key value (hex w/o leading 0x). The key should be minimum 8 characters in length.
	• esp <256-4294967295> – Configures an *Encapsulating Security Payload* (ESP) key. Specify the ESP key SPI between 256 - 4294967295.
	  • cipher <WORD> – Specify the security association key value (hex w/o leading 0x). The key should be minimum 8 characters in length.
	  • authenticator <WORD> – Specify the ESP key autehnticator.

transform-set <WORD>	Assigns a transform-set to this crypto map • <WORD> – Specify the transformset to use.

Usage Guidelines

```
RFS7000(config-crypto-map)#set peer (name)
```

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first; then the new peer IP address can be configured.

```
RFS7000(config-crypto-map)#set pfs
```

If left at the default setting, no *perfect forward secrecy* (PFS) will be used during IPSec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data linkage between prior keys and future keys.

```
RFS7000(config-crypto-map)#set security-association lifetime (kilobytes|seconds)
```

Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the security association.

```
RFS7000(config-crypto-map)#set session-key (inbound|outbound)(ah|esp)
RFS7000(config-crypto-map)#set session-key (inbound|outbound) ah <hexkey data>
```

```
RFS7000(config-crypto-map)#set session-key (inbound|outbound) esp <SPI> cipher <hexdata
key> authenticator <hexkey data>
```

The inbound local SPI (security parameter index) must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

They are not true ASCII strings. Therefore, a key of 3031323334353637 represents “01234567”.

```
RFS7000(config-crypto-map)#set transformset (name)
```

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms.

If no transform-set is configured for a crypto map, then the entry is incomplete and will have no effect on the system. For manual key crypto maps, only one transform set can be specified.

Example

```
RFS7000(config-crypto-map)#set localid hostname TestMapHost
```

10.1.9 show

Crypto Map Config Commands

Use this command to view the current system information that is running on the switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
RFS7000(config-crypto-map)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-crypto-map)#
```

11

Crypto - trustpoint Instance

Use the `config-trustpoint` commands to define a *Certificate Authority* (CA) trustpoint.

This is a separate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance. To instantiate the `crypto-trustpoint` instance, use the following command:

```
RFS7000(config)#crypto pki trustpoint <TRUSTPOINT-NAME>
RFS7000(config-trustpoint)#
```

11.1 Trustpoint Config commands

Table 11.1 summarizes the **`config-crypto-trustpoint`** commands.

Table 11.1 Truspoint (PKI) Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 11-2*
company-name	Defines a company name (applicable only for request) for the trustpoint	*page 11-3*
email	Sets an e-mail ID for the trustpoint	*page 11-4*
end	Ends the current mode and moves to the EXEC mode	*page 11-5*
exit	Ends the current mode and moves to the previous mode	*page 11-6*
fqdn	Sets the domain name for the trustpoint	*page 11-7*
help	Describes the interactive help system	*page 11-8*
ip-address	Configures *Internet Protocol* (IP) address fo rthe trustpoint	*page 11-9*
no	Negates a command or sets its defaults	*page 11-10*
password	Sets the challenge password (applicable only by request) to access the trustpoint	*page 11-11*
rsakeypair	Defines an RSA Keypair to associate with the trustpoint	*page 11-12*
service	Displays service commands	*page 11-13*
show	Shows the running system information	*page 11-14*
subject-name	Configures the subject name for this trustpoint. The subject name is a collection of required parameters to configure a trustpoint.	*page 11-16*

11.1.1 clrscr

Trustpoint Config commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-trustpoint)#clrscr
RFS7000(config-trustpoint)#
```

11.1.2 company-name

Trustpoint Config commands

Use this command to set the company name (applicable only by request) to a trustpoint.

Syntax

```
company-name <WORD>
```

Parameters

<WORD>	Specify the company name (2 - 64 characters in length).

Usage Guidelines

The company name defined must be between 2 - 64 characters only.

Example

```
RFS7000(config-trustpoint)#company-name RetailKing
RFS7000(config-trustpoint)#
```

11.1.3 email

Trustpoint Config commands

Use this command to configure an e-mail address for this trustpoint.

Syntax

```
email <WORD>
```

Parameters

<WORD>	Specify the e-mail address (2 - 64 characters in length).

Usage Guidelines

The e-mail address defined must be between of 2 - 64 characters only.

Example

```
RFS7000(config-trustpoint)#email abcTestemailID@motorolasolutions.com
RFS7000(config-trustpoint)#
```

11.1.4 end

Trustpoint Config commands

Use this command to end and exit the `(config-trustpoint)` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-trustpoint)#end
RFS7000#
```

11.1.5 exit

Trustpoint Config commands

Use this command to end the `(config-trustpoint)` mode and move to previous GLOBAL CONFIG mode.The prompt now changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-trustpoint)#exit
RFS7000(config)#
```

11.1.6 fqdn

Trustpoint Config commands

Use this command to configure the *fully qualified domain name* (fqdn) for this trustpoint.

Syntax

```
fqdn <WORD>
```

<WORD>	Specify the domain name (9 - 64 characters in length).

Usage Guidelines

The string length of the domain name must be between 9 - 64 characters.

Example

```
RFS7000(config-trustpoint)#fqdn RetailKing.com
RFS7000(config-trustpoint)#
```

11.1.7 help

Trustpoint Config commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-trustpoint)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-trustpoint)#
```

11.1.8 ip-address

Trustpoint Config commands

Use this command to configure an IP address for the trustpoint.

Syntax

```
ip-address <A.B.C.D>
```

Parameters

<A.B.C.D>	Enter the the trustpoint's IP address.

Example

```
RFS7000(config-trustpoint)#ip-address 157.200.200.02
RFS7000(config-trustpoint)#
```

11.1.9 no

Trustpoint Config commands

Use this command to negate a command or set defaults.

Syntax

```
no [company-name|email|fqdn|ip-address|subject-name]
```

Parameters

company-name	Negates the configured company name
email	Negates the configured e-mail address
fqdn	Negates the configured *Domain Name Configuration* (DNS)
ip-address	Negates the configured *Internet Protocol* (IP) address
subject-name	Negates subject name, which is a collection of required parameters to configure a trustpoint (it comprises of common_name, country, state, organization,org name etc.)

Example

```
RFS7000(config-trustpoint)#no ip-address
RFS7000(config-trustpoint)#
```

11.1.10 password

Trustpoint Config commands

Use this command to set the challenge password, applicable only for trustpoint access requests.

Syntax

```
password [0 <WORD>|2 <WORD>|<WORD>]
```

Parameters

0 <WORD>	Password is specified as UNENCRYPTED. The password must be between 4 - 20 characters length.
2 <WORD>	Password is encrypted with a password-encryption secret. The string length of an encrypted password must be between 4 - 20 characters in length.
<WORD>	The password (4 - 20 characters)

Example

```
RFS7000(config-trustpoint)#password 0 TestPassword
RFS7000(config-trustpoint)#
```

11.1.11 rsakeypair

Trustpoint Config commands

Use this command to configure a RSA Keypair to associate with the trustpoint.

Syntax

```
rsakeypair <WORD>
```

Parameters

<WORD>	Specify the RSA keypair identifier.

Usage Guidelines

Use RSA Key Pair support to configure the switch to have *Rivest, Shamir, and Adelman* (RSA) key pairs. The switch software can maintain a different key pair for each identity certificate.

Example

```
RFS7000(config-trustpoint)#rsakeypair were
RFS7000(config-trustpoint)#
```

The `rsakeypair` name `were` in this example is an exisitng keypair value.

11.1.12 service

Trustpoint Config commands

Use this command to invoke service commands to troubleshoot or debug `crypto pki trustpoint` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows the CLI tree of current mode

Example

```
RFS7000(config-trustpoint)#service show cli
Trustpoint Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-trustpoint)#
```

11.1.13 show

Trustpoint Config commands

Use this command to view current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-trustpoint)#show ?
 aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-trustpoint)#

RFS7000(config)#show crypto pki trustpoints
Trustpoint :TRUSTPOINT1
-----------------------------------------------

Trustpoint :TestTrustpoint
-----------------------------------------------

Trustpoint :default-trustpoint
-----------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:         Motorola
      Organizational Unit: EWLAN
      Organization:        Enterprise Mobility
      Location:            San Jose
      State:               CA
      Country:             US
    Issuer Name:
      Common Name:         Motorola
      Organizational Unit: EWLAN
      Organization:        Enterprise Mobility
      Location:            San Jose
 -- MORE --, next page: Space, next line: Enter, quit: Control-CRFS7000(config)#


RFS7000(config-trustpoint)#show access-list
Standard IP access list 1
    mark tos 0 host 1.2.3.4 log rule-precedence 1
Extended IP access list 100
    deny icmp any any rule-precedence 10
Standard IP access list 1300
    deny host 1.2.3.4 rule-precedence 1
Extended MAC access list MACACL1
Extended IP access list TestList

RFS7000(config-trustpoint)#

RFS7000(config-trustpoint)#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
** 1       cli    172.16.10.12      00:00m      Nov  2 12:48:32 2011

RFS7000(config-trustpoint)#

RFS7000(config-trustpoint)#show users
 Line     PID      User        Uptime       Location
 130 vty 0  5253   admin       00:04m       0

RFS7000(config-trustpoint)#

RFS7000(config-trustpoint)#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Oct 29 18:32:17 2011
RFS7000(config-trustpoint)#
```

11.1.14 subject-name

Trustpoint Config commands

Use this command to create a subject name to configure a trustpoint. A subject name is a collection of required parameters.

Syntax

```
subject-name <Name> [<Country>] [<State>] [<City>] [<Organisation>] [<Org Unit>]
```

Parameters

WORD	The subject name is a collection of required parameters to configure a trustpoint. It consists of the common_name, country, state, org name etc. • Name – Enter the trustpoint name. The string can have a maximum of 64 characters. • Country – Enter the 2 character ISO country code. • State – Enter the state name. The string can have a maximum of 128 characters. • City – Enter the city name. The string can have a maximum of 128 characters. • Organization – Enter the organization name. The string can have a maximum of 64 characters. • Organization Unit – Enter the organization unit name. The string can have a maximum of 64 characters.

Example

```
RFS7000(config-trustpoint)#subject-name TestPool ?
  WORD  Country ( 2 character ISO Code )

RFS7000(config-trustpoint)#subject-name TestPool US ?
  WORD  State( 2 to 128 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH ?
  WORD  City( 2 to 128 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH PB ?
  WORD  Organization( 2 to 64 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH PB MOTOROLA ?
  WORD  Organization Unit( 2 to 64 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH PB MOTOROLA WID ?
  <cr>

RFS7000(config-trustpoint)#subject-name TestPool US OH PB MOTOORLA WID
RFS7000(config-trustpoint)#
```

12

Interface Instance

Use the **(config-if)** instance to configure the following interfaces: FastEthernet (fe), GigaEhternet (ge), StaticAggregate interface (sa), and VLAN.
To instantiate the (config-if) mode, use the following commands:

```
RFS7000(config)#interface [<INTERFACE-NAME>|ge <1-4>|sa <1-4>|vlan <1-4094>]
RFS7000(config-if)#
```

12.1 Interface Config commands

Table 12.1 summarizes the **config-if** commands.

Table 12.1 Interface Config Command Summary

Command	Description	Ref.
clrsc r	Clears the display screen	*page 12-3*
crypto	Configures the encryption module	*page 12-4*
description	Configures the interface specific description	*page 12-5*
duplex	Defines the duplex mode of operation	*page 12-6*
end	Ends the current mode and moves to the EXEC mode	*page 12-7*
exit	Ends the current mode and moves down to the previous mode	*page 12-8*
help	Describes the interactive help system	*page 12-9*
ip	Configures an IP address for the assigned Ethernet or VLAN	*page 12-10*
mac	Applies MAC access list to a GigabitEthernet interface	*page 12-12*
management	Sets the selected interface as the management interface	*page 12-13*
no	Negates a command or sets its defaults	*page 12-14*
port-channel	Configures the load-balancing criteria of a aggregated port	*page 12-15*
service	Invokes service commands to trouble shoot or debug the `(config-if)` instance	*page 12-16*
show	Shows the running system information	*page 12-17*
shutdown	Shuts down the selected interface	*page 12-19*
spanning-tree	Configures spanning tree parameters	*page 12-20*

Table 12.1 Interface Config Command Summary

Command	Description	Ref.
speed	Configures the speed of a FastEthernet port (10/100) or a GigabitEthernet port (10/100/1000)	*page 12-22*
static-channel-group	Configures static channel commands	*page 12-23*
storm-control	Configures broadcast/multicast/unicast rate limits for the interface	*page 12-26*
switchport	Sets switching mode characteristics	*page 12-24*

12.1.1 clrscr

Interface Config commands

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-if)#clrscr
RFS7000(config-if)#
```

12.1.2 crypto

Interface Config commands

Use this command to assign a crypto map to a specified interface.

Syntax

```
crypto map <CRYPTO-MAP-NAME>
```

Parameters

crypto map	Configures a crypto map for the specified interface
<CRYPTO-MAP-NAME>	Specify the crypto map to associate with this interface (the cyprto map should exist)

Example

```
RFS7000(config-if)#crypto map test
% Error: Invalid Remote Peer
RFS7000(config-if)#
```

12.1.3 description

Interface Config commands

Use this command to create an interface specific description.

Syntax

```
description <LINE>
```

Parameters

<LINE>	Enter a description for this interface.

Example

```
RFS7000(config-if)#description "interface for RetailKing"
RFS7000(config-if)#
```

12.1.4 duplex

Interface Config commands

Use this command to specify the duplex mode of operation on the specified interface.

NOTE

- Duplexity can only be set for an Ethernet type interface. Enter the `(config-if)` instance using an `ge/me` parameter in an `interface` mode.
- Duplex cannot be set until the speed is set to a non-auto value.

Syntax

```
duplex [auto|full|half]
```

Parameters

auto	Sets the auto-negotiate mode of operation. In this mode, the duplex is selected based on the connected network hardware.
full	Sets the full-duplex mode of operation. In this mode, data can be passed in both direction simultaneously.
half	Sets the half-duplex mode of operation. In this mode, data can be passed only in one direction at a time.

Usage Guidelines

Duplex defines the type of communication used by the port. The switch, by default, is set as `auto` duplex. In auto mode the duplex is selected based on the connected network hardware.

Example

```
RFS7000(config)#interface ge 4

RFS7000(config-if)#duplex ?
  auto  set auto-negotiate
  full  set full-duplex
  half  set half-duplex

RFS7000(config-if)#duplex full
RFS7000(config-if)#
```

12.1.5 end

Interface Config commands

Use this command to exit the `(config-if)` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-if)#end
RFS7000#
```

12.1.6 exit

Interface Config commands

Use this command to end the `(config-if)` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-if)#exit
RFS7000(config)#
```

12.1.7 help

Interface Config commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-if)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-if)#
```

12.1.8 ip

Interface Config commands

Use this command to configure an IP address for the assigned Ethernet, or VLAN.

Syntax

```
ip [access-group|address|arp|dhcp|helper-address|nat]

ip access-group [<1-99>|<100-199>|<1300-1999>|<2000-2699>|<WORD>] in
ip address [<A.B.C.D/M>|dhcp]
ip address [<A.B.C.D/M>] {secondary}
ip arp [rate-limit <1-1000000>|trust]
ip dhcp [trust]
ip helper-address <A.B.C.D>
ip nat [inside|outside]
```

Parameters

access-group [<1-99>|<100-199>| <1300-1999>| <2000-2699>]	Configures an *access control list* (ACL) on this interface • [<1-99>|<1300-1999>] – Configures an IP standard access list • [<100-199>|<2000-2699>] – Configures an IP extended access list (expanded range) • <WORD> – Configures the specified access list. Specify the access list name. • in – Applies the ACL to incoming packets
address [<A.B.C.D/M>|dhcp]	Sets a static IP address and network mask of a Layer3 SVI (Switch Virtual Interface) • A.B.C.D/M – Specify the IP address (for example, 10.0.0.1/8). • secondary – The secondary IP address • dhcp – Uses a DHCP client to obtain an IP address for the interface (this enables DHCP on the Layer3 SVI)
arp [rate-limit <1-1000000> |trust]	Configures *Address Resolution Protocol* (ARP) ratelimiting on this interface • rate-limit <1-1000000> – Ratelimits packets at the rate of <1-1000000> packets per second • trust – Enables the trust state for ARP responses on this interface
dhcp [trust]	Configures DHCP trust state on this interface • trust – Enables the trust state for DHCP responses on this interface
helper-address <A.B.C.D>	Enables forwarding of DHCP and BOOTP packets • <A.B.C.D> – Specify the IP address to which DHCP and BOOTP packets are forwarded.
nat	Configures *Network Address Translation* (NAT) on this interface • inside – The inside interface • outside – The outside interface

Usage Guidelines

IPv4 commands are not allowed on a L2 interface. Use the `ip access-group` command to attach an access list to an interface. Use the `no ip access-group` command to remove the access list from the interface.

Use `mac access-group` to attach a MAC access list to an interface.

Use the `[no] ip [options]` command to undo all the above IP based interface configurations.

Example

```
RFS7000(config-if)#ip access-group 110 in
RFS7000(config-if)#

RFS7000(config-if)#ip address 192.168.234.1/24
RFS7000(config-if)#
```

Follow the steps in the example below to create a helper address on VLAN 2000 for using the DHCP server available on VLAN 1000:

```
RFS7000(config)#interface vlan 1000
RFS7000(config-if)#ip address 172.168.100.1/24

RFS7000(config-if)#interface vlan 2000
RFS7000(config-if)#ip address 172.168.200.1/24

RFS7000(config-if)#ip helper-address 172.168.100.10 vlan 1000
RFS7000(config-if)#
```

The example below displays static NAT source translation.

```
RFS7000(config)#interface vlan 1000
RFS7000(config-if)#ip nat inside

RFS7000(config-if)#interface vlan 2000
RFS7000(config-if)#ip nat outside

RFS7000(config)#ip nat inside source static 172.168.200.10 157.235.205.57
RFS7000(config)#
```

12.1.9 mac

Interface Config commands

Use this command to apply a MAC access list to a GigabitEthernet interface.

NOTE Access list cannot be applied on a management interface (me1).

Syntax

```
mac [access-group <ACL-NAME>] (in)
```

Parameters

access-group <ACL-NAME>	Sets MAC access groups ACL • <ACL-NAME> – Specify the MAC ACL name.
in	Applies the MAC ACL to ingress packets

Example

```
RFS7000(config-if)#mac access-group Ark200 in
RFS7000(config-if)#
```

12.1.10 management

Interface Config commands

Use this command to configure the selected interface as the management interface. It can only be used on a VLANx interface. The tftp/ftp server, which provides the switch its config file at startup, must be accessible via this interface.

VLAN 1 is the default management interface for the RFS7000 switch.

Syntax

```
management
```

Parameters

None

Usage Guidelines

Management privilege can be set only on a L3 interface. Use this command along with the `(config) management secure` in config mode. This ensures switch management access is restricted to the management VLAN only.

Refer *management on page 5-52* for `(config) management secure` configuration.

Example

```
RFS7000(config)#interface vlan 1000
RFS7000(config-if)#management
RFS7000(config-if)#
```

12.1.11 no

Interface Config commands

Use this command to negate a command or set defaults.

Syntax

```
no [crypto|description|duplex|ip|mac|port-channel|shutdown|
   spanning-tree|speed|static-channel-group|storm-control|switchport]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFS7000(config-if)#no mtu
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree link-type
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree portfast
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree portfast bpdu-guard
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree portfast bpdu-filter
RFS7000(config-if)#
```

12.1.12 port-channel

Interface Config commands

Use this command to select the load-balance criteria of an aggregated port.

Syntax

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

Parameters

load-balance [src-dst-ip|src-dst-mac]	Sets load-balancing for port channel • src-dst-ip – Enables source and destination IP address based load balancing • src-dst-mac – Enables source and destination MAC address based load balancing

Usage Guidelines

Use this command to configure and set the load balance to the aggregated port using `(config-if) static-channel-group`.

Example

The example below creates a channel group 1 with interface ge1 and ge2.

```
RFS7000(config)#interface ge1
RFS7000(config-if)#static-channel-group 1

RFS7000(config)#interface ge2
RFS7000(config-if)#static-channel-group 1
```

The example below defines the load balance based on the IP or MAC address.

```
RFS7000(config)#interface sa1
RFS7000(config-if)#port-channel load-balance src-dst-ip
RFS7000(config-if)#
```

12.1.13 service

Interface Config commands

Use this command to invoke service commands to troubleshoot or debug the `(config-if)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show	Shows running system information
cli	Shows the CLI tree of current mode

Example

```
RFS7000(config-if)#service show cli
Interface Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
]...............................................................................
...............................................................................
...............................................................................
...............................................................................
..............
RFS7000(config-if)#
```

12.1.14 show

Interface Config commands

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-if)#show ?
  aap-wlan-acl           wlan based acl
   aap-wlan-acl-stats    IP filtering wlan based statistics
   access-banner         Display Access Banner
   access-list           Internet Protocol (IP)
   aclstats              Show ACL Statistics information
   alarm-log             Display all alarms currently in the system
   audit-log-filters     Display audit log filter rules
   autoinstall           autoinstall configuration
   boot                  Display boot configuration.
   clock                 Display system clock
   commands              Show command lists
   crypto                encryption module
   crypto-error-log      Display Crypto Error Log
   crypto-log            Display Crypto Log
   debugging             Debugging information outputs
   dhcp                  DHCP Server Configuration
   environment           show environmental information
   file                  Display filesystem information
   firewall              Wireless firewall
   history               Display the session command history
   interfaces            Interface status
   ip                    Internet Protocol (IP)
   ldap                  LDAP server
   licenses              Show any installed licenses
   logging               Show logging configuration and buffer
   mac                   Internet Protocol (IP)
   mac-address-table     Display MAC address table
   mac-name              Displays the configured MAC Names
   management            Display L3 Managment Interface name
   mobility              Display Mobility parameters
   ntp                   Network time protocol
   password-encryption   password encryption
   port                  Physical/Aggregate port interface
   port-channel          Portchannel commands
   privilege             Show current privilege level
   protocol-list         List of protocols
   radius                RADIUS configuration commands
   redundancy            Configure redundancy group parameters
   role                  Configure role parameters
   rtls                  Real Time Locating System commands
   running-config        Current Operating configuration
   securitymgr           Securitymgr parameters
   service-list          List of services
   sessions              Display current active open connections
   smtp-notification     Display SNMP engine parameters
   snmp                  Display SNMP engine parameters
   snmp-server           Display SNMP engine parameters
   spanning-tree         Display spanning tree information
   startup-config        Contents of startup configuration
   static-channel-group  static channel group membership
   terminal              Display terminal configuration parameters
   timezone              Display timezone
   traffic-shape         Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-if)#show

RFS7000(config-if)#show boot

Image           Build Date              Install Date           Version
-----       --------------------    --------------------      --------------
Primary     Sep 24 06:24:14 2011     unknown                  4.1.2.0-007GD
Secondary   Sep 24 06:24:14 2011     unknown                  4.1.2.0-007GD

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled

RFS7000(config-if)#

RFS7000(config-if)#show wireless config
country-code             : us
adoption-pref-id         : 1
proxy-arp                : enabled
adopt-unconf-radio       : enabled
ap-detection             : disabled
manual-wlan-mapping      : disabled
dhcp sniff state         : disabled
dhcp one portal forward : disabled
dhcp fix broadcast-rsp  : disabled
broadcast-tx-speed       : optimize-for-range
wlan bw allocation       : disabled
smart-channels used      : 1,6,11,36,40,44,48,149,153,157,161,165
smart-channels excluded : 2,3,4,5,7,8,9,10
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
user load balance mode  : disabled

admission control for voice : disabled
cluster-master-support      : enabled
nas-id                      : ""
nas-port-id                 : ""

wired-to-wireless rate limit per user : unlimited
wireless-to-wired rate limit per user : unlimited

RFS7000(config-if)#

RFS7000(config-if)#show spanning-tree mst
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 800000157037fdf5
% 1: CIST Reg Root Id 800000157037fdf5
% 1: CST Bridge Id 800000157037fdf5
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability configured - Current cisco interoperability off
%
%   Instance        VLAN
%   0:              1-4095
RFS7000(config-if)#
```

12.1.15 shutdown

Interface Config commands

Use this command to shutdown/disable the selected interface. The interface is administratively enabled unless explicitly disabled using this command.

Syntax

```
shutdown
```

Parameters

None

Example

```
RFS7000(config-if)#shutdown
RFS7000(config-if)#
```

12.1.16 spanning-tree

Interface Config commands

Use this command to configure spanning tree parameters.

Syntax

```
spanning-tree [bpdufilter|bpduguard|edgeport|force-version|guard|link-type|mst|portfast]

spanning-tree [bpdufilter (enable|disable)|bpduguard (disable|enable)|edgeport|
  force-version <0-3>|guard (root)|link-type (point-to-point|shared)|
  mst [<0-15>|port-cisco-interoperability]|portfast]

spanning-tree mst [<0-15> (cost <1-200000000>|port-priority <0-240>)|
  port-cisco-interoperability (disable|enable)]
```

Parameters

bpdufilter (disable|enable)	Use this command to set a portfast *Bridge Protocol Data Unit* (BPDU) filter for the port. Use the no parameter with this command to revert the port BPDU filter to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFastenabled ports do not transmit or receive BPDUs.
bpduguard (disable|enable)	Use this command to enable or disable the BPDU guard feature on a port. Use the no parameter with this command to set the BPDU guard feature to default values. When BPDU guard is set for a bridge, all portfast-enabled ports that have BPDU guard set to default shut down the port upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after the specified interval.
edgeport	Enables an interface as an edgeport
force-version <0-3>	Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: • 0 – *Spanning Tree Protocol* (STP) • 1 – Not supported • 2 – *Rapid Spanning Tree Protocol* (RSTP) • 3 – *Multiple Spanning Tree Protocol* (MSTP) The default value for forcing the version is MSTP.
guard (root)	Enables the root guard feature for the port. The root guard disables the reception of superior BPDUs. The root guard ensures the enabled port is a designated port. If the root guard enabled port receives a superior BPDU, it moves to a discarding state. Use the no parameter with this command to disable the root guard feature.
link-type (point-to-point|shared)	Enables or disables point-to-point or shared link types • point-to-point – Enables rapid transition • shared – Disables rapid transition

mst [<0-15> (cost <1-200000000>| port-priority <0-240>)| port-cisco-interoperability (disable|enable)]	Configures MST on a spanning tree
	• <0-15> – Specifies the instance ID
	  • cost <1-200000000> – Configures the path cost for a port between 1 - 200000000 (lower path costs indicate higher chances of becoming root)
	  • port-priority <0-240> – Configures the port priority for a bridge in increments of 16. Specify the port priority between 0 - 240 (lower port priority indicates higher chances of becoming root)
	• port-cisco-interoperability (disable|enable) – Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP)
	  • enable – Enables CISCO Interoperability
	  • disable – Disables CISCO Interoperability
	The default is `disabled`.

portfast	Enables rapid transitions

Example

```
RFS7000(config-if)#spanning-tree edgeport
RFS7000(config-if)#

RFS7000(config-if)#spanning-tree guard root
RFS7000(config-if)#

RFS7000(config-if)#spanning-tree link-type point-to-point
RFS7000(config-if)#

RFS7000(config-if)#spanning-tree link-type shared
RFS7000(config-if)#
```

12.1.17 speed

Interface Config commands

Use this command to specify the speed of a FastEthernet (10/100) or a GigabitEthernet port (10/100/1000).

Syntax

```
speed [010|100|1000|auto]
```

Parameters

10	Forces 10 Mbps operation. The port runs at 10 Mbps.
100	Forces 100 Mbps operation.The port runs at 100 Mbps.
1000	Forces 1000 Mbps operation.The port runs at 1000 Mbps.
auto	Enables AUTO speed configuration.The port automatically detects the speed it should run based on the port at the other end of the link.

Usage Guidelines

Set the interface speed to `auto` to detect and use the fastest speed available. The speed detection is based on the connected network hardware.

Example

```
RFS7000(config-if)#speed auto
RFS7000(config-if)#

RFS7000(config-if)#speed 1000
RFS7000(config-if)#

RFS7000(config-if)#show interfaces ge2
Interface ge2
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fb-73
  index=2002, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin 1G, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 767, bytes 144486, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
RFS7000(config-if)#
```

12.1.18 static-channel-group

Interface Config commands

Use this command to add an interface to a static channel group.

Syntax

```
static-channel-group <1-4>
```

Parameters

<1-4>	The static channel group to associate the link with

Usage Guidelines

This command aggregates individual Giga port's into a single aggregate link to provide a larger bandwidth. The static channel group is used to provide additional bandwidth in multiples of 1Gbps on the switch. All MAC layer and higher protocols see only the static channel group (aggregate link) rather than the individual ports that comprise it.

Example

```
RFS7000(config-if)#static-channel-group 2
RFS7000(config-if)#
```

12.1.19 switchport

Interface Config commands

Use this command to set switching mode characteristics for the selected interface. The mode can be either access or trunk.

NOTE A `ge` interface configured as a trunk with *all* VLAN's allowed looses its configuration and has only VLAN 1 set to allowed.

Syntax

```
switchport [access|mode|trunk]

switchport access vlan <1-4094>
switchport mode [access|trunk]
switchport trunk(allowed|native)
switchport trunk allowed vlan [add <VLAN-ID>|none|remove <VLAN-ID>]
switchport trunk native [tagged|vlan <1-4094>]
```

Parameters

access vlan <1-4094>	Configures the access VLAN of an access-mode port • vlan <1-4094> – Sets the access VLAN ID, when an interface is in the access mode
mode (access|trunk)	Sets the interface's switching mode to access or trunk. The switching mode can be used only on physical (Layer2) interfaces. • access – If `access mode` is selected, the access VLAN will be automatically set to VLAN1. In this mode, only untagged packets in the access VLAN (VLAN1) will be accepted on this port. All tagged packets will be discarded. • trunk – If `trunk` mode is selected tagged packets in all VLANs will be accepted. The native VLAN will be automatically set to VLAN1. Untagged packets will be placed in the native VLAN by the switch. Outgoing packets in the native VLAN will be sent out untagged. The default mode for both ports is `trunk`.

trunk (allowed|native)	Sets trunking mode characteristics
	• allowed vlan [add <VLAN-ID>|none|remove <VLAN-ID>] – Configures trunk characteristics when the port is in thetrunk mode.
	  • vlan add <VLAN-ID> – Adds VLANs to the current list
	  • vlan none – Allows no VLANs to transmit or receive through the L2 interface
	  • vlan remove <VLAN-ID> – Removes VLANs to the current list
	• native [tagged|vlan <1-4094>] – Configures the native VLAN ID of the trunk-mode port
	  • tagged – Tags the native VLAN
	  • vlan <1-4094> – Configures the native VLAN for classifying untagged traffic. Specify the native VLAN ID between 1 - 4094.

Usage Guidelines

The interface ge1-ge4 can be configured either as trunk or in access mode. An interface configured as trunk allows packets from the given list of VLANs added to the trunk. Interfaces configured as *access* allow packets only from the native VLANs.

Use `[no] switchport (access|mode|trunk)` to undo the above switchport configurations.

Example

```
RFS7000(config-if)#switchport mode access
RFS7000(config-if)#
```

12.1.20 storm-control

Interface Config commands

Use this command to configure storm control parameters.

Syntax

```
storm-control [bcast|mcast|ucast] rate-limit <1-1000000>
```

Parameters

storm-control	Configures rate limits for broadcast, multicast, and unicast traffic
bcast rate-limit <1-1000000>	Configures packet rate limiting for broadcast traffic • <1-1000000> – Configures the allowed rate between 1 - 1000000 packets per second
mcast rate-limit <1-1000000>	Configures packet rate limiting for multicast traffic • <1-1000000> – Configures the allowed rate between 1 - 1000000 packets per second
ucast rate-limit <1-1000000>	Configures packet rate limiting for unicast traffic • <1-1000000> – Configures the allowed rate between 1 - 1000000 packets per second

Example

```
RFS7000(config-if)#storm-control bcast rate-limit 1000
RFS7000(config-if)#
```

13

Spanning Tree-MST Instance

Use the **(config-mst)** instance to configure the *Multi Spanning Tree Protocol* (MSTP). Use the command `spanning-tree mst configuration` to instantiate this instance.

13.1 MST Config commands

Table 13.1 summarizes the **config-mst** commands.

Table 13.1 MSTP Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 13-2*
end	Ends the current mode and moves to the EXEC mode	*page 13-3*
exit	Ends the current mode and moves to the previous mode	*page 13-4*
help	Describes the interactive help system	*page 13-5*
instance	Assigns a VLAN to the bridge instance	*page 13-6*
name	Sets a name for the MST region	*page 13-7*
no	Negates a command or sets defaults	*page 13-8*
revision	Configures the revision number of the MST bridge	*page 13-9*
service	Displays service commands	*page 13-10*
show	Shows running system information	*page 13-11*

13.1.1 clrscr

MST Config commands

Use this command to clear the display.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-mst)#clrscr
RFS7000(config-mst)#
```

13.1.2 end

MST Config commands

Use this command to end and exit from the `(config-mst)` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-mst)#end
RFS7000#
```

13.1.3 exit

MST Config commands

Use this command to end the `(config-mst)` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-mst)#exit
RFS7000(config)#
```

13.1.4 help

MST Config commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-mst)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-mst)#
```

13.1.5 instance

MST Config commands

Use this command to associate VLAN(s) with an MST instance.

Syntax

```
instance <1-15> vlan <VLAN_ID>
```

Parameters

<1-15>	Defines the MST instance ID to which the VLAN is associated
vlan <VLAN_ID>	Defines the VLAN ID for association with this MST instance

Usage Guidelines

Multiple Spanning Tree Protocol (MSTP) configuration is based on instances. An instance is a group of VLAN's with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Switches with same instance - VLAN mapping, revision number and region names create a region. Switches in the same region exchange *bridge protocol data units* (BPDU) with instance record information.

Example

The example below creates an instance named 10 and maps VLAN 20 to it.

```
RFS7000(config-mst)#instance 10 vlan 20
RFS7000(config-mst)#
```

13.1.6 name

MST Config commands

Use this command to set a name for the MST region.

Syntax

```
name [<LINE>]
```

Parameters

<LINE>	Specify the MST region name.

Example

```
RFS7000(config-mst)#name MyRegion
RFS7000(config-mst)#

RFS7000(config-mst)#show spanning-tree mst configuration
%
%  MSTP Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : MyRegion
%  Revision Level : 0
%  Digest         : 0xE3E3A9F4A0BDDF5D9BF8A50356866B98
%-------------------------------------------------------
RFS7000(config-mst)#
```

13.1.7 no

MST Config commands

Use this command to negate a command or set defaults.

Syntax

```
no [instance|name|revision]
no [instance <1-15>] [vlan <VLAN_ID>]
```

Parameters

instance <1-15> vlan <VLAN_ID>	Removes the VLAN(s) associated with the MST instance specified by the <1-15> MST instance ID • vlan <VLAN_ID> – Removes the VLAN(s) specified by the <VLAN_ID> parameter
name	Removes the MST region name
revision	Removes the revision number for configuration information

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFS7000(config-mst)#no instance 10 vlan 20
RFS7000(config-mst)#

RFS7000(config-mst)#no name
RFS7000(config-mst)#

RFS7000(config-mst)#no revision
RFS7000(config-mst)#
```

13.1.8 revision

MST Config commands

Use this command to configure the revision number of the MST bridge.

Syntax

```
revision <0-255>
```

Parameters

<0-255>	Specify the revision number for configuration information between 0 - 255.

Example

```
RFS7000(config-mst)#revision 20
RFS7000(config-mst)#

RFS7000(config-mst)#show spanning-tree mst configuration
%
%  MSTP Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 20
%  Digest         : 0xAC36177F50283CD4B83821D8AB26DE62
%-------------------------------------------------------
RFS7000(config-mst)#
```

13.1.9 service

MST Config commands

Use this command to invoke the service commands needed to troubleshoot or debug `(config-if)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows running system information • cli – Shows CLI tree of current mode

Example

```
RFS7000(config-mst)#service show cli
MSTI configuration mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-mst)#service show cli
MSTI configuration mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
-- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-mst)#
```

13.1.10 show

MST Config commands

Use this command to view current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the `show` command

Example

```
RFS7000(config-mst)#show ?aap-wlan-acl          wlan based acl
aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-mst)#

RFS7000(config-mst)#show wlan-acl all
WLAN port: 102
  Inbound IP Access List : 110
  Inbound MAC Access List :

  Outbound IP Access List:
  Outbound MAC Access List :
RFS7000(config-mst)#

RFS7000(config-mst)#show access-banner
This Device is running in Common Criteria Mode
Attention:
This is a protected and private wireless system. No un-authorized access allowed.
You must have proper rights to access and manage this system from the authorized
personnel.
RFS7000(config-mst)#
```

13.2 Configuring Interface using MSTP

MSTP is enabled by default. All VLANs are in the default instance 0 by default.

1. Use the following command to create a non-default instance and region configuration using the `mst config` mode:

   ```
   RFS7000(config-mst)#instance 1 vlan <vlan-id>
   ```

2. Use the following to enable/disable MSTP:

   ```
   RFS7000(config)#bridge multiple-spanning-tree
   ```

3. Use the following command to configure spanning-tree:

   ```
   RFS7000(config)#bridge multiple-spanning-tree
   RFS7000(config)#spanning-tree
   ```

4. Use the following command to configure spanning-tree for ports:

   ```
   RFS7000(config-if)#spanning-tree
   ```

14

Extended ACL Instance

Use the **(config-ext-nacl)** instance to configure **ip access-list extended** ACLs.

Extended access lists are statements that deny or permit packets based on the specified source/destination IP address, port numbers, and upper layer protocols. Standard access lists deny/permit packets by source IP address only. The destination address and the port involved are not specified in the list.

14.1 Extended ACL Config Commands

Table 14.1 summarizes the **config-ext-nacl** commands.

Table 14.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	*page 14-2*
deny	Specifies packets to reject.	*page 14-3*
end	Ends the current mode and changes to the EXEC mode.	*page 14-8*
exit	Ends the current mode and moves back to the previous mode.	*page 14-9*
help	Displays the interactive help system.	*page 14-10*
mark	Specifies packets to mark.	*page 14-11*
no	Negates a command or set default values.	*page 14-17*
permit	Specifies packets to forward.	*page 14-18*
service	Service commands.	*page 14-24*
show	Shows running system information.	*page 14-25*

14.1.1 clrscr

Extended ACL Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#clrscr
RFS7000(config-ext-nacl)#
```

14.1.2 deny

Extended ACL Config Commands

Use this command to specify packets to reject.

Syntax

```
deny [icmp|ip|proto|tcp|udp]

deny ip [<SOURCE-IP/MASK>|host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|host <A.B.C.D>|any]
  {log} {(rule-description <DESCRIPTION>|rule-precedence <1-5000>)}

deny icmp [<SOURCE-IP/MASK>|host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|host <A.B.C.D>|
  any] {<ICMP-TYPE>|<ICMP-CODE>} {log} {rule-description <DESCRIPTION>|
  rule-precedence <1-5000>)}

deny proto [<1-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] [<SOURCE-IP/MASK>|
  host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|host <A.B.C.D>|any]
  {log} {(rule-description <DESCRIPTION>|rule-precedence <1-5000>)}

deny [tcp|udp] [<SOURCE-IP/MASK>|host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|
  host <A.B.C.D>|any|eq <1-65535>|range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT>]
{log} {(rule-description <DESCRIPTION>|rule-precedence <1-5000>)}
```

Parameters

deny (ip)	

[<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/MASK>| host <A.B.C.D>|any] {log} {(rule-description <DESCRIPTION>| rule-precedence <1-5000>)}	Use the **deny ip** command to reject IP packets from a specified source or to a specified destination.
	Define the network or host to deny as a source of packets, using one of the following options:
	• <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
	• any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0.
	• host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32.
	Define the network or host to deny as a destination of packets, using one of the following options:
	• <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format.
	• any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0.
	• host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32.
	The following keywords are common to all of the above:
	• log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	  • rule-description <DESCRIPTION> – Optional. Describes this IP deny ACL rule (should not exceed 128 characters in length).
	  • rule-precedence <1-500> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

deny (icmp)	
[<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/MASK>| host <A.B.C.D>|any] <ICMP-TYPE> <ICMP-CODE> {log} {(rule-description <DESCRIPTION>| rule-precedence <1-500)}	Use the **`deny icmp`** command to reject *Internet Control Message Protocol* (ICMP) packets. Define the network or host to deny as a source of packets, using one of the following options: • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32. Define the network or host to deny as the destination of packets, using one of the following options: • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact destination IP address and destination-mask bits equal to 32. The following keywords are common to all of the above: • <ICMP-TYPE> – Optional. Specify the ICMP type value from 0 - 255. • <ICMP-CODE> – Optional. Specify the ICMP code value from 0 - 255. **Note:** The ICMP type field identifies the ICMP message and the ICMP code field provides more information about the associated TYPE field. • log – Optional. Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this ICMP deny ACL rule (should not exceed 128 characters in length). • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

deny (proto)	

[<1-254>|<WORD>|
eigrp|gre|igmp|
igp|ospf|vrrp]
[<SOURCE-IP/MASK>|
host <A.B.C.D>|any]
[<DESTINATION-IP/MASK>|
host <A.B.C.D>|any]
{log}
{(rule-description
<DESCRIPTION>|
rule-precedence
<1-5000>)}
	Use the **`deny proto`** command to reject packets other than IP, ICMP, TCP, and UDP.
	• <1-254> – Filters protocols using their *Internet Assigned Numbers Authority* (IANA) protocol number. Specify the protocol number between 1 - 254.
	• <WORD> – Filters protocols using their IANA protocol name. Use the `show protocol-list` command to view protocol names & corresponding numbers.
	• eigrp – Identifies the *Enhanced Internet Gateway Routing Protocol* (EIGRP) protocol (88).
	• gre – Identifies the *General Routing Encapsulation* (GRE) protocol (47).
	• igmp – Identifies the *Internet Group Management Protocol* (IGMP) protocol (2).
	• igp – Identifies any private internal gateway (primarily used by CISCO for their IGRP) (9).
	• ospf – Identifies the *Open Shortest Path First* (OSPF) protocol (89).
	• vrrp – Identifies the *Virtual Router Redundancy Protocol* (VRRP) protocol (112).
	Define the network or host to deny as a source of packets using one of the following options:
	• <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
	• any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0.
	• host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32.
	Define the network or host to deny as a destination of packets using one of the following options:
	• <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format.
	• any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0.
	• host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32.
	The following keywords are common to all of the above:
	• log – Optional. Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs.
	  • rule-description <DESCRIPTION> – Optional. Describes this proto deny ACL rule (should not exceed 128 characters in length).
	  • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

deny (tcp|udp)	
[<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/ MASK>|host <A.B.C.D>| any|eq <1-65535>| range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT>] [operator destination-port] {log} {rule-description <DESCRIPTION>| rule-precedence <1-5000>}	Use the **`deny [tcp|udp]`** command to reject TCP or UDP packets. • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32. • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact destination IP address and destination-mask bits equal to 32. • eq <1-65535> – Matches a specific source port. Specify the TCP/UDP source port value between 1 - 65535. • range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT> – Matches a range of source ports. Specify the range by providing the starting and ending source port values. The following keywords are common to all of the above: [operator destination-port] – Specifies the destination port. Valid only for the TCP and UDP protocols. Valid values are eq and range. • eq <1-65535> – Optional. Matches a specific destination port. Specify the TCP/UDP destination port value between 1 - 65535. • range <STARTING-DESTINATION-PORT> <ENDING-DESTINATION-PORT> – Optional. Matches a range of destination ports. Specify the range by providing the starting and ending destination port values. • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this TCP/UDP deny ACL rule (should not exceed 128 characters in length). • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

Usage Guidelines

Use this command to deny traffic between network's/host's based on the protocol type selected in the access list configuration. The following protocol types are supported:

- IP
- ICMP
- TCP
- UDP

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

- Filtering on protocol types TCP/UDP allows the user to specify port numbers as filtering criteria.
- Select ICMP to allow/deny ICMP packets. Selecting ICMP provides the option of filtering ICMP packets based on ICMP type and code.

NOTE The log option is functional only for router ACL's. The log option displays an informational logging message for the packet that matches the entry sent to the console.

Example

The following example denies traffic between two subnets:

```
RFS7000(config-ext-nacl)#deny ip 192.168.2.0/24 192.168.1.0/24
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

The following example denies TCP traffic with source port range between 20 - 23 from the source subnet to destination sub net:

```
RFS7000(config-ext-nacl)#deny tcp 192.168.1.0/24 192.168.2.0/24 range 20 23
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

The following example denies UDP traffic with a source port range between 20 - 23 from the source subnet to destination sub net.

```
RFS7000(config-ext-nacl)#deny udp 192.168.1.0/24 192.168.2.0/24 range 20 23
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

The following example denies ICMP traffic from any source to any destination. The keyword *any* is used to match any source or destination IP address.

```
RFS7000(config-ext-nacl)#deny icmp any any
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

14.1.3 end

Extended ACL Config Commands

SyntaxUse this command to end and exit the `config-ext-nacl` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#.`

```
end
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#end
RFS7000#
```

14.1.4 exit

Extended ACL Config Commands

Use this command to end the `config-ext-nacl` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#exit
RFS7000(config)#
```

14.1.5 help

Extended ACL Config Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-ext-nacl)#
```

14.1.6 mark

Extended ACL Config Commands

Use this command to mark specific packets.

Syntax

```
mark [8021p|dscp|tos] [icmp|ip|proto|tcp|udp]

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [ip] [SOURCE-IP/MASK|host <A.B.C.D>|any]
  [<DESTINATION-IP/MASK>|host <A.B.C.D>|any] {log} {rule-precedence access-list-entry
precedence}

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [icmp] [SOURCE-IP/MASK|host <A.B.C.D>|any]
  [<DESTINATION-IP/MASK>|host <A.B.C.D>|any] {<ICMP-TYPE> <ICMP-CODE>}
  {log} {rule-description <DESCRIPTION>|rule-precedence <1-5000>}
mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [proto] [<1-254>|<WORD>|eigrp|
  gre|igmp|igp|ospf|vrrp] [SOURCE-IP/MASK|host <A.B.C.D>|any]
  [<DESTINATION-IP/MASK>|host <A.B.C.D>|any]
  {log} {rule-description <DESCRIPTION>|rule-precedence <1-5000>}

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [tcp|udp] [SOURCE-IP/MASK|host <A.B.C.D>|any]
  [<DESTINATION-IP/MASK>|host <A.B.C.D>|any] [operator destination-port] {log} {rule-
description <DESCRIPTION>|rule-precedence <1-5000>}
```

Parameters

mark [8021p <0-7>| dscp <0-63>| tos <0-255>]	Use the **mark** command to specify IP packets to mark.
	• mark [8021p <0-7>|dscp <0-63>|tos <0-255>] – The keyword specifies mark action on an ACL. The action type mark is functional only over a Port ACL.
	  • 8021p <0-7> – Used only with action type mark to specify 8021p VLAN user priority.
	  • dscp <0-63> – Modifies DSCP TOS bits in the IP header. Specify the DSCP codepoint value between 0 - 63.
	  • tos <0-255> – Used only with action type mark to specify *Type of Service* (tos) bits in the IP header. (least significant 2 bits must be given a tos value of 0)

mark [8021p <0-7> | dscp <0-63>| tos <0-255>] IP	
[ip] [<SOURCE-IP/MASK>| host <A.B.C.D>|any] <DESTINATION-IP/ MASK>| host <A.B.C.D>|any] {log} {rule-description <DESCRIPTION>| rule-precedence <1-500>}	Specifies IP as the protocol to match. • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for the exact source IP address and source-mask bits equal to 32. • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32. The following keywords are common to all of the above: • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this IP mark packets rule (should not exceed 128 characters in length). • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

mark [8021p <0-7> | dscp <0-63>| tos <0-255>] icmp	
[icmp] [<SOURCE-IP/MASK>| host <A.B.C.D>|any] <DESTINATION-IP/ MASK>| host <A.B.C.D>|any] {<ICMP-TYPE>| <ICMP-CODE>} {log} {rule-description <DESCRIPTION>| rule-precedence <1-500>}	Specifies ICMP as the protocol to match. • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for the exact source IP address and source-mask bits equal to 32. • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32.The following keywords are common to all of the above: The following keywords are common to all of the above: • <ICMP-TYPE> – Optional. The ICMP type value from 0 - 255. Valid only for ICMP protocol. • <ICMP-CODE> – Optional. The ICMP code value from 0 - 255. Valid only for ICMP protocol. • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this ICMP mark packets rule (should not exceed 128 characters in length). • [rule-precedence <1-5000>] – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

mark [8021p <0-7> | dscp <0-63>| tos <0-255>] [tcp|udp]	
[tcp|udp] [<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/ MASK>| host <A.B.C.D>| any|eq <1-65535>| range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT>] [operator destination-port] {log} {rule-description <DESCRIPTION>| rule-precedence <1-5000>}	Specifies TCP or UDP as the protocol to match. • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32. • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact destination IP address and destination-mask bits equal to 32. • eq <1-65535> – Matches a specific source port. Specify the TCP/UDP source port value between 1 - 65535. • range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT> – Matches a range of source ports. Specify the range by providing the starting and ending source port values. The following keywords are common to all of the above: [operator destination-port] – Specifies the destination port. Valid only TCP and UDP protocols. Valid values are eq and range. • eq <1-65535> – Optional. Matches a specific destination port. Specify the TCP/UDP destination port value between 1 - 65535. • range <STARTING-DESTINATION-PORT> <ENDING-DESTINATION-PORT> – Optional. Matches a range of destination ports. Specify the range by providing the starting and ending destination port values. • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this TCP/UDP mark packets rule (should not exceed 128 characters in length). • [rule-precedence <1-5000>] – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

mark [8021p <0-7> | dscp <0-63>| tos <0-255>] proto	

proto [<1-254>|<WORD>| eigrp|gre|igmp|igp| ospf|vrrp] [<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/ MASK>| host <A.B.C.D>|any] {log} {rule-description <DESCRIPTION>| rule-precedence <1-5000>}	Specifies any protocol other than IP, ICMP, TCP, and UDP.
	• <1-254> – Specify the protocol number to match between 1 - 254.
	• <WORD> – Specify the protocol name. Use the `show protocol-list` command to list the protocol names and corresponding numbers.
	• eigrp – Specifies EIGRP protocol (88)
	• gre – Specifies GRE protocol (47)
	• igmp – Specifies IGMP protocol (2)
	• igp – Specifies IGP protocol (9)
	• ospf – Specifies OSPF protocol (890
	• vrrp – Specifies VRRP protocol (112)
	  • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
	  • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0.
	  • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32.
	  • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format.
	  • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0.
	  • host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32.
	The following keywords are common to all of the above:
	• log – Optional. Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs.
	  • rule-description <DESCRIPTION> – Optional. Describes this proto mark packets rule (should not exceed 128 characters in length).
	  • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

Usage Guidelines

This command marks traffic between network's/host's based on the protocol type selected in the access list configuration.

Use the `mark` option to specify the *type of service* (tos) and priority values. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

The following types of protocols are supported:

- IP
- ICMP
- TCP
- UDP

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is marked based on the ACL configuration.

- Filtering on protocol types TCP/UDP allows the user to specify port numbers as filtering criteria.
- Select the protocol type ICMP to allow/deny ICMP packets. Selecting ICMP protocol allows you to filter ICMP packets based on the ICMP type and code.

NOTE The log option is functional only for router ACL's. The log option provides an informational logging message about the packet matching the entry sent to the console.

Example

The example below marks the dot1p priority value in the Ethernet header to 5 to all TCP traffic coming from the source subnet.

```
RFS7000(config-ext-nacl)#mark 8021p 5 tcp 192.168.2.0/24 any
RFS7000(config-ext-nacl)#
```

The example below marks the tos value in the IP header to 245 to all TCP traffic coming from the source subnet.

```
RFS7000(config-ext-nacl)#mark tos 245 tcp 192.168.2.0/24 any
RFS7000(config-ext-nacl)#
```

14.1.7 no

Extended ACL Config Commands

Use this command to negate a command or set its defaults.

Syntax

```
no [deny|mark|permit]
```

This command negates all the syntax combinations used in *deny*, *mark* and *permit* commands to configure the Extended ACL.

Parameters

no deny	Negates the deny packets rule entry in an IP extended ACL.
no mark	Negates the mark packets rule entry in an IP extended ACL.
no permit	Negates the permit packets rule entry in an IP extended ACL.

Usage Guidelines

Use the `no` command to remove an access list control entry. Provide the rule-precedence value when using the no command.

Example

```
RFS7000(config-ext-nacl)#no mark 8021p 5 tcp 192.168.2.0/24 any rule-precedence 10
RFS7000(config-ext-nacl)#

RFS7000(config-ext-nacl)#no permit ip any any rule-precedence 10
RFS7000(config-ext-nacl)#

RFS7000(config-ext-nacl)#no deny icmp any any rule-precedence 10
RFS7000(config-ext-nacl)#
```

14.1.8 permit

Extended ACL Config Commands

Use this command to permit specific packets.

NOTE ACLs do not allow DHCP messages to flow by default. Configure an Access Control Entry (ACE) to allow DHCP messages to flow through.

```
RFS7000(config-ext-nacl)#permit ip 192.168.1.0/24 192.168.2.0/24
RFS7000(config-ext-nacl)#permit ip any host 255.255.255.255
RFS7000(config-ext-nacl)#
```

Syntax

```
permit [icmp|ip|proto|tcp|udp]

permit ip [<SOURCE-IP/MASK>|host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|host <A.B.C.D>|
  any] {log} {(rule-description <DESCRIPTION>|rule-precedence <1-5000>)}

permit icmp [<SOURCE-IP/MASK>|host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|host <A.B.C.D>|
  any] {<ICMP-TYPE>|<ICMP-CODE>} {log} {rule-description <DESCRIPTION>|
  rule-precedence <1-5000>)}

permit proto [<1-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] [<SOURCE-IP/MASK>|
  host <A.B.C.D>|any] [<DESTINATION-IP/MASK>|host <A.B.C.D>|any]
  {log} {(rule-description <DESCRIPTION>|rule-precedence <1-5000>)}
```

Parameters`permit [tcp|udp] [<SOURCE-IP/MASK>|host <A.B.C.D>|any] [<DESTINATION-IP/MASK>| host <A.B.C.D>|any|eq <1-65535>|range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT>] {log} {(rule-description <DESCRIPTION>|rule-precedence <1-5000>)}`

permit (ip)	
[<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/MASK>| host <A.B.C.D>|any] {log} {(rule-description <DESCRIPTION>| rule-precedence <1-5000>)}	Use the **permit ip** command to allow IP packets. Defines the network or host to permit as a source of packets,. Use one of the following options to provide the network/host IP address: • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32. Define the network or host to permit as a destination of packets, using one of the following options: • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32. The following keywords are common to all of the above: • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this IP permit ACL rule (should not exceed 128 characters in length). • rule-precedence <1-500> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

permit (icmp)	
[<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/MASK>| host <A.B.C.D>|any] <ICMP-TYPE> <ICMP-CODE> {log} {(rule-description <DESCRIPTION>| rule-precedence <1-500)	Use the **`permit icmp`** command to allow ICMP packets. Define the network or host to permit as a source of packets, using one of the following options: • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32. Define the network or host to permit as the destination of packets, using one of the following options: • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact destination IP address and destination-mask bits equal to 32. The following keywords are common to all of the above: • <ICMP-TYPE> – Optional. Specify the ICMP type value from 0 - 255. • <ICMP-CODE> – Optional. Specify the ICMP code value from 0 - 255. **Note:** The ICMP type field identifies the ICMP message and the ICMP code field provides more information about the associated TYPE field. • log – Optional. Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this ICMP permit ACL rule (should not exceed 128 characters in length). • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

permit [tcp|udp]	
[<SOURCE-IP/MASK>| host <A.B.C.D>|any] [<DESTINATION-IP/MASK>| host <A.B.C.D>| any|eq <1-65535>| range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT>] [operator destination-port] {log} {rule-description <DESCRIPTION>| rule-precedence <1-5000>}	Use the **`permit [tcp|udp]`** command to allow TCP or UDP packets. • <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32. • <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format. • any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0. • host <A.B.C.D> – Is an abbreviation for exact destination IP address and destination-mask bits equal to 32. • eq <1-65535> – Matches a specific source port. Specify the TCP/UDP source port value between 1 - 65535. • range <STARTING-SOURCE-PORT> <ENDING-SOURCE-PORT> – Matches a range of source ports. Specify the range by providing the starting and ending source port values. The following keywords are common to all of the above: [operator destination-port] – Specifies the destination port. Valid only for the TCP and UDP protocols. Valid values are eq and range. • eq <1-65535> – Optional. Matches a specific destination port. Specify the TCP/UDP destination port value between 1 - 65535. • range <STARTING-DESTINATION-PORT> <ENDING-DESTINATION-PORT> – Optional. Matches a range of destination ports. Specify the range by providing the starting and ending destination port values. • log – Optional. Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-description <DESCRIPTION> – Optional. Describes this TCP/UDP permit ACL rule (should not exceed 128 characters in length). • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

permit (proto)	

[<1-254>|<WORD>|
eigrp|gre|igmp|
igp|ospf|vrrp]
[<SOURCE-IP/MASK>|
host <A.B.C.D>|any]
[<DESTINATION-IP/MASK>|
host <A.B.C.D>|any]
{log}
{(rule-description
<DESCRIPTION>|
rule-precedence
<1-5000>)}
	Use the **`permit proto`** command to allow packets other than IP, ICMP, TCP, and UDP.
	• <1-254> – Filters protocols using their *Internet Assigned Numbers Authority* (IANA) protocol number. Specify the protocol number between 1 - 254.
	• <WORD> – Filters protocols using their IANA protocol name. Use the `show protocol-list` command to view protocol names & corresponding numbers.
	• eigrp – Identifies the *Enhanced Internet Gateway Routing Protocol* (EIGRP) protocol (88).
	• gre – Identifies the *General Routing Encapsulation* (GRE) protocol (47).
	• igmp – Identifies the *Internet Group Management Protocol* (IGMP) protocol (2).
	• igp – Identifies any private internal gateway (primarily used by CISCO for their IGRP) (9).
	• ospf – Identifies the *Open Shortest Path First* (OSPF) protocol (89).
	• vrrp – Identifies the *Virtual Router Redundancy Protocol* (VRRP) protocol (112).
	Define the network or host to permit as a source of packets using one of the following options:
	• <SOURCE-IP/MASK> – The IP address and mask of the source network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
	• any – Is an abbreviation for any source IP address of 0.0.0.0 and source-mask bits equal to 0.
	• host <A.B.C.D> – Is an abbreviation for exact source IP address and source-mask bits equal to 32.
	Define the network or host to permit as a destination of packets using one of the following options:
	• <DESTINATION-IP/MASK> – The IP address and mask of the destination network or host in dotted decimal format.
	• any – Is an abbreviation for any destination IP address of 0.0.0.0 and destination-mask bits equal to 0.
	• host <A.B.C.D> – Is an abbreviation for the exact destination IP address and destination-mask bits equal to 32.
	The following keywords are common to all of the above:
	• log – Optional. Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs.
	  • rule-description <DESCRIPTION> – Optional. Describes this proto permit ACL rule (should not exceed 128 characters in length).
	  • rule-precedence <1-5000> – Optional. Integer value between 1- 5000 that sets the rule precedence in the ACL.

Usage Guidelines

Use this command to permit traffic between network's/host's based on the protocol type selected in the access list configuration. The following protocols are supported:

- IP
- ICMP
- TCP
- UDP

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed based on the ACL configuration.

- Filtering on Protocol types TCP/UDP allows the user to specify port numbers as filtering criteria.
- Select the protocol type ICMP to allow ICMP packets. Selecting ICMP allows filtering of ICMP packets based on the ICMP type and code.

NOTE The log option is functional only for router ACL's. The log option causes an informational logging message about the packet matching the entry sent to the console.

Example

The example below allows IP traffic from the source subnet to destination subnet and denies all other traffic over an interface.

```
RFS7000(config-ext-nacl)#permit ip 192.168.1.10/24 192.168.2.0/24 rule-precedence 40
RFS7000(config-ext-nacl)#
```

The example below allows ICMP based traffic and denies all other traffic over an interface.

```
RFS7000(config-ext-nacl)#permit icmp any any rule-precedence 30
RFS7000(config-ext-nacl)#)#
```

14.1.9 service

Extended ACL Config Commands

Use this command to invoke service commands to troubleshoot or debug **(config-if)** instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows CLI tree of current mode.

Example

```
RFS7000(config-ext-nacl)#service show cliExtended ACL Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
    +-dhcp
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-ext-nacl)#
```

14.1.10 show

Extended ACL Config Commands

Use this command to view the current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

The `show access-list` command displays all the access lists configured in the switch console. Provide the access list name or number to view the details of a particular ACL.

Example

```
RFS7000(config-ext-nacl)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  audit-log-filters      Display audit log filter rules
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information

  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands


  role                   Configure role parameters
  rtls                   Real Time Locating System command
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
```

```
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-ext-nacl)#show

RFS7000(config-ext-nacl)#show access-list
Extended IP access list 101
    deny ip 192.168.1.0/24 192.168.2.0/24 rule-precedence 10
    permit ip any any rule-precedence 20
Extended IP access list 110
    deny ip host 192.168.1.95 host 192.168.2.98 log rule-precedence 10
    permit ip any any rule-precedence 20
Extended IP access list symbol
    deny tcp 192.168.2.0/24 192.168.1.0/24 rule-precedence 10
    permit ip any any rule-precedence 20
RFS7000(config-ext-nacl)#
```

15

Standard ACL Instance

Use the **(config-std-nacl)** instance to configure **ip access-list standard** ACLs. Standard ACLs allow filtering based on the source address only.

15.1 Standard ACL Config Commands

Table 15.1 summarizes **config-std-nacl** commands.

Table 15.1 Standard ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	*page 15-2*
deny	Specifies packets to reject.	*page 15-3*
end	Ends the current mode and changes to EXEC mode.	*page 15-4*
exit	Ends the current mode and moves to the previous mode.	*page 15-5*
help	Displays the interactive help system.	*page 15-6*
mark	Specifies packets to mark.	*page 15-7*
no	Negates a command or set its defaults.	*page 15-8*
permit	Specifies packets to forward.	*page 15-9*
service	Displays service commands.	*page 15-10*
show	Shows the running system information.	*page 15-11*

15.1.1 clrscr

Standard ACL Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#clrscr
RFS7000(config-std-nacl)#
```

15.1.2 deny

Standard ACL Config Commands

Use this command to specify packets to reject.

Syntax

```
deny [<SOURCE-IP/MASK>|any|host <A.B.C.D>] {log (rule-precedence <1-500>)}
deny [<SOURCE-IP/MASK>|any|host <A.B.C.D>] {rule-precedence <1-500>}
```

Parameters

<SOURCE-IP/MASK>	The source IP address range to match. Rejects packets from the source specified by the <SOURCE-IP/MASK> parameter.
any	Specifies a source IP address and mask of value 0.0.0.0 and 255.255.255.255.
host <A.B.C.D>	Specifies the IP address of a single host. Rejects packets from the specified host. • <A.B.C.D> – The exact source IP address to match.
log	Optional. Logs matches against this entry.
rule-precedence <1-500>	Optional. Configures the precedence of this entry in this standard ACL.

Usage Guidelines

Use this command to deny traffic based on the source (defined by the IP address or network address). The last *access control entry* (ACE) in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

NOTE The log option is functional only for router ACL's. The log option results in an informational logging message for the packet matching the entry sent to the console.

Example

The example below denies all traffic entering the interface. A log message is generated in the console whenever the interface receives a packet.

```
RFS7000(config-std-nacl)#deny any log rule-precedence 50
RFS7000(config-std-nacl)#
```

The example below denies traffic from the source network (xxx.xxx.1.0/24) and allows all other traffic to flow through the interface.

```
RFS7000(config-std-nacl)#deny xxx.xxx.1.0/24 rule-precedence 60
RFS7000(config-std-nacl)#permit any
```

15.1.3 end

Standard ACL Config Commands

Use this command to exit the `config-std-nacl` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#.`

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#end
RFS7000#
```

15.1.4 exit

Standard ACL Config Commands

Use this command to end the `config-std-nacl` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#exit
RFS7000(config)#
```

15.1.5 help

Standard ACL Config Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFS7000(config-std-nacl)#
```

15.1.6 mark

Standard ACL Config Commands

Use this command to mark specific packets.

Syntax

```
mark [8021p <0-7>|dscp <0-63>|tos <0-255>]

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [<SOURCE-IP/MASK>|any|host <A.B.C.D>]
  {log (rule-precedence <1-500>)}

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [<SOURCE-IP/MASK>|any|host <A.B.C.D>]
  {rule-precedence <1-500>}
```

Parameters

[8021p <0-7>| dscp <0-63>| tos <0-255>]	Specifies one of the following user priority types: • 8021p <0-7> – Used only with action type `mark` to specify 8021p VLAN user priority between 0 - 7. • dscp <0-63> – Used only with action type `mark` to specify DSCP TOS bits value between 0 and 63. • tos <0-255> – Used only with action type `mark` to specify *Type of Service* (tos) bits in the IP header. (least significant 2 bits must be given a tos value of 0).
<SOURCE-IP/MASK>	Marks packets received form a specified source. • <SOURCE-IP/MASK> – The IP address of the source network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
any	Marks packets received fromIs an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
host	Is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
log	Optional. Logs matches against this entry.
rule-precedence <1-500>	Optional. Configures the precedence of this entry in this standard ACL.

Usage Guidelines

UUse this command to mark traffic from the source network/host. Use the mark option to specify the *type of service* (tos) and priority value. The tos value is marked in the IP header. The 802.1p priority value is marked in the frame.

r When the interface receives the packet, its content is checked against the ACE's in the ACL. It is marked based on the ACL configuration.

NOTE The log option is functional only for router ACL's. The log option results in an informational logging message about the packet matching the entry sent to the console.

Example

The example below marks the *type of service* (tos) value to 254 for all traffic coming from the source network.

```
RFS7000(config)#access-list 3 mark tos 254 xxx.xxx.3.0/24
 RFS7000(config)#access-list 3 permit any
```

15.1.7 no

Standard ACL Config Commands

Use this command to negate a command or set its defaults.

Syntax

```
no [deny|mark|permit]
```

Usage Guidelines

no deny	Negates the deny packets rule entry in a standard ACL
no mark	Negates the mark packets rule entry in a standard ACL.
no permit	Negates the permit packets rule entry in a standard ACL

Use the `no` command to remove an access list control entry. Provide the rule-precedence value when using the `no` command.

```
RFS7000(config-std-nacl)#no permit any rule-precedence 10
RFS7000(config-std-nacl)#

RFS7000(config-std-nacl)#no deny any rule-precedence 20
RFS7000(config-std-nacl)#

RFS7000(config-std-nacl)#no mark tos 4 192.168.2.0/24 rule-precedence 30
RFS7000(config-std-nacl)#
```

15.1.8 permit

Standard ACL Config Commands

Use this command to permit specific packets.

Syntax

```
permit [<SOURCE-IP/MASK>|any|host <A.B.C.D>] {log (rule-precedence <1-500>)}
```

Parameters`permit [<SOURCE-IP/MASK>|any|host <A.B.C.D>] {rule-precedence <1-500>}`

<SOURCE-IP/MASK>	The source IP address range to match. Forwards packets from the source specified by the <SOURCE-IP/MASK> parameter.
any	Specifies a source IP address and mask of value 0.0.0.0 and 255.255.255.255.
host <A.B.C.D>	Specifies the IP address of a single host. Forwards packets from the specified host specified by the <A.B.C.D> parameter. • <A.B.C.D> – The exact source IP address to match.
log	Optional. Logs matches against this entry.
rule-precedence <1-500>	Optional. Configures the precedence of this entry in this standard ACL.

Use this command to allow traffic based on the source IP address or network address. The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed based on the ACL configuration.

NOTE The log option is functional only for router ACL's. The log option outputs an informational logging message about the packet matching the entry sent to the console.

Example

The example below permits all traffic to the interface.

```
RFS7000(config-std-nacl)#permit any rule-precedence 50
RFS7000(config-std-nacl)#
```

The example below permits traffic from the source network and provides a log message.

```
RFS7000(config-std-nacl)#permit xxx.xxx.1.0/24 log rule-precedence 60
RFS7000(config-std-nacl)#
```

15.1.9 service

Standard ACL Config Commands

Use this command to invoke service commands to troubleshoot or debug **(config-if)** instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows CLI tree of current mode.

Example

```
RFS7000(config-std-nacl)#service show cliStandard ACL Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
    +-dhcp
      +-binding [show ip dhcp binding]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-std-nacl)#
```

15.1.10 show

Standard ACL Config Commands

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Usage Guidelines

The `show access-list` command displays all the access lists configured in the switch console. Provide the access list name or number to view the details of a particular ACL.

Example

```
RFS7000(config-std-nacl)#show ?aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
```

```
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-std-nacl)#show

RFS7000(config-std-nacl)#show access-list
Standard IP access list 1
Standard IP access list 10
Extended IP access list 100
    deny ip 1.2.3.4/24 2.5.6.8/11 rule-precedence 10 rule-description "test"
    deny ip any any rule-precedence 20 rule-description "This is a test extended access
list"
    deny tcp host 1.2.3.4 5.6.7.8/11 rule-precedence 30
    mark tos 0 proto vrrp host 1.2.3.4 host 3.4.5.6 rule-precedence 40
    mark tos 0 proto igmp any any rule-precedence 50
    permit ip 1.2.3.4/24 any rule-precedence 60 rule-description "test"
    permit icmp any any log rule-precedence 70 rule-description "testICMPpermit"
    permit proto 254 1.2.2.3/23 5.6.7.8/11 log rule-precedence 80
Extended IP access list 2000
    deny ip any any rule-precedence 10
Extended MAC access list MACacl1
    deny any any type 8021q rule-precedence 1
RFS7000(config-std-nacl)#
```

16

Extended MAC ACL Instance

Use the **(config-ext-macl)** instance to configure **mac access-list extended** ACLs associated with the switch.

Use a decimal value representation of Ethertypes to implement `permit/deny/mark` packet. The command set for Extended MAC ACLs provides hexadecimal values for each of its listed ethertypes. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed in the CLI for any other ethertype.

16.1 MAC Extended ACL Config Commands

Table 16.1 summarizes the **config-ext-macl** commands.

Table 16.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	*page 16-2*
deny	Specifies packets to reject.	*page 16-3*
end	Ends the current mode and changes to EXEC mode.	*page 16-6*
exit	Ends the current mode and moves to the previous mode.	*page 16-7*
help	Displays the interactive help system.	*page 16-8*
mark	Specifies packets to mark.	*page 16-9*
no	Negates a command or set its defaults.	*page 16-11*
permit	Specifies packets to forward.	*page 16-12*
service	Displays service commands.	*page 16-15*
show	Shows the running system information.	*page 16-16*

16.1.1 clrscr

MAC Extended ACL Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#clrscr
RFS7000(config-ext-macl)#
```

16.1.2 deny

MAC Extended ACL Config Commands

Use this command to specify packets to reject.

NOTE Use a decimal value representation of ethertypes to implement a `permit/deny/mark` designation for a packet. The command set for Extended MAC ACLs provides hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed or for any other type of ethertype.

Syntax

```
deny [<SOURCE-MAC/MASK>|any|host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-MAC/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] {dot1p [<0-7>]|rule-precedence [<1-5000>]|type [<OPTION>]|
  vlan [<1-4095>]}

deny [<SOURCE-MAC/MASK>|any|host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-MAC/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] {dot1p [<0-7>] {rule-precedence <1-5000>|type [<OPTION>]
  rule-precedence <1-5000>}}

deny [<SOURCE-MAC/MASK>|any|host <AA.BB.CC.DD.EE.FF] [<DESTINATION-MAC/MASK>|any|
  host <AA.BB.CC.DD.EE.FF>] {type <OPTION> {rule-precedence <1-5000>}}

deny [<SOURCE-MAC/MASK>|any|host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-MAC/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] {vlan <1-4095> {rule-precedence <1-5000>|
  type <OPTION> rule-precedence <1-5000>}}
```

Parameters

[<SOURCE-MAC/MASK|any| host <XX:XX:XX:XX:XX:XX>]	Use the `deny` command to reject packets from a specified source network/host and to a specified network/host. Rejects packets to the specified source MAC addresses. The source wildcard can be any one of the following: • <SOURCE-MAC/MASK> – The source MAC address and mask in the xx.xx.xx.xx.xx.xx/xx.xx.xx.xx.xx.xx format. • any – Specifies any source host. • host <XX:XX:XX:XX:XX:XX> – Specifies the exact source MAC address to match.
[<DESTINATION-MAC/MASK|any| host <XX:XX:XX:XX:XX:XX>]	Rejects packets to the specified destination MAC addresses. The destination wildcard can be any one of the following: • <DESTINATION-MAC/MASK> – The destination MAC address and mask in the xx.xx.xx.xx.xx.xx/xx.xx.xx.xx.xx.xx format. • any – Specifies any source host. • host <XX:XX:XX:XX:XX:XX> – Specifies the exact destination MAC address to match.
dot1p <0-7>	Optional. The 802.1p priority value to match.
rule-precedence <1-5000>	Optional. The MAC access list entry precedence.

type <OPTION>	Optional. The Ethertype value represented as integer or keywords for well known Ethertypes.The options are: • 8021q – Specifies VLAN Ethertype (0x8100) • <1-65535> – Specifies an Ethernet protocol number • aarp – Specifies *AppleTalk Address Resolution Protocol* (AARP) Ethertype (0x80F3) • appletalk – Specifies APPLETALK Ethertype (0x809B) • arp – Specifies *Address Resolution Protocol* (ARP) Ethertype (0x0806) • ip – Specifies IP Ethertype (0x800) • ipv6 – Specifies IPv6 Ethertype (0x86DD) • ipx – Specifies IPX Ethertype (0x8137) • rarp – Specifies *Reverse Address Resolution Protocol* (RARP) Ethertype (0x8035) • wisp – Specifies WISP Ethertype (0x8783)
vlan <1-4095>	Optional. The VLAN tag ID to match.

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) information. The MAC access list denies traffic from a particular source MAC address or any MAC address. It also has an option to disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can be configured to disallow traffic based on VLAN information and ethernet type.

The most common ethernet type are:

- AARP
- AppleTalk
- RARP
- ARP
- WISP
- IP
- 802.1q

By default, the switch does not allow layer 2 traffic to pass through the interface. To adopt access port through an interface, configure an access control list to allow an ethernet wisp.

NOTE A MAC access list entry to allow arp is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

Example

The MAC AC (in the example below) denies traffic from any source MAC address to a particular host MAC address.

```
RFS7000(config-ext-macl)#deny any host 00:01:ae:00:22:11
RFS7000(config-ext-macl)#
```

The MAC ACL (in the example below) denies dot1q tagged traffic from VLAN interface 5.

```
RFS7000(config-ext-macl)#deny any any vlan 5 type 8021q
RFS7000(config-ext-macl)#
```

The example below denies traffic between two hosts based on MAC addresses.

```
RFS7000(config-ext-macl)#deny host 01:02:fe:45:76:89 host 01:02:89:78:78:45
RFS7000(config-ext-macl)#
```

16.1.3 end

MAC Extended ACL Config Commands

Use this command to exit from the `config-ext-macl` mode and change to PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#end
RFS7000#
```

16.1.4 exit

MAC Extended ACL Config Commands

Use this command to end the `config-ext-macl` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#exit
RFS7000(config)#
```

16.1.5 help

MAC Extended ACL Config Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-ext-macl)#
```

16.1.6 mark

MAC Extended ACL Config Commands

Use this command to specify a packet to mark.

NOTE Use a decimal value representation of Ethertypes to implement `permit/deny/mark` designations for a packet. The command set for an Extended MAC ACL provides hexadecimal values for each of its listed Ethertypes. The switch supports all Ethertypes. Use the decimal equvilant of the Ethertype listed in the CLI or for any other type of Ethertype.

Syntax

```
mark [8021p|dscp|tos]

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [<SOURCE-IP/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-IP/MASK>|any|host <XX:XX:XX:XX:XX:XX>]

mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [<SOURCE-IP/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-IP/MASK>|any|host <XX:XX:XX:XX:XX:XX>]
  {dot1p|rule-precedence <1-1500>|type <OPTION>|vlan <1-4095>}
```

Parameters

mark [8021p <0-7>| dscp <0-63>| tos <0-255>]	Use the **`mark`** command to specify IP packets to mark. • mark [8021p <0-7>|dscp <0-63>|tos <0-255>] – The keyword specifies mark action on an ACL. The action type `mark` is functional only over a Port ACL. • 8021p <0-7> – Used only with action type `mark` to specify 8021p VLAN user priority. • dscp <0-63> – Modifies DSCP TOS bits in the IP header. Specify the DSCP codepoint value between 0 - 63. • tos <0-255> – Used only with action type `mark` to specify *Type of Service* (tos) bits in the IP header. (least significant 2 bits must be given a tos value of 0)
[<SOURCE-IP/MASK>|any| host <XX:XX:XX:XX:XX:XX>]	Bit mask specifying the bits to match. The source wildcard can be any one of the following: • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx – Source MAC address and mask. • any – Any source host. • host – Exact source MAC address to match.
[<DESTINATION-IP/MASK>|any| host <XX:XX:XX:XX:XX:XX>]	Bit mask specifying the bits to match. The destination wildcard can be any one of the following: • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx – Destination MAC address and mask. • any – Any destination host. • host – Exact destination MAC address to match.
dot1p <0-7>	Optional. The VLAN 802.1p priority value to match.
rule-precedence <1-5000>	Optional. The access list entry precedence value.

type <OPTION> {rule-precedence <1-5000>}	Optional. Ethertype value represented as integer or keywords for well-known ethertypes.The options are: • 8021q – Specifies VLAN Ethertype (0x8100) • <1-65535> – Specifies an Ethernet protocol number • aarp – Specifies *AppleTalk Address Resolution Protocol* (AARP) Ethertype (0x80F3) • appletalk – Specifies APPLETALK Ethertype (0x809B) • arp – Specifies *Address Resolution Protocol* (ARP) Ethertype (0x0806) • ip – Specifies IP Ethertype (0x800) • ipv6 – Specifies IPv6 Ethertype (0x86DD) • ipx – Specifies IPX Ethertype (0x8137) • rarp – Specifies *Reverse Address Resolution Protocol* (RARP) Ethertype (0x8035) • wisp – Specifies WISP Ethertype (0x8783) • rule-precedence <1-5000> – Optional. The access list entry precedence value.

Usage Guidelines

Use the mark option to specify the *type of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is marked based on the ACL configuration.

Example

The following example marks the dot1p priority value to 6 for all 802.1q tagged traffic from VLAN interface 5:

```
RFS7000(config-ext-macl)#mark 8021p 6 any any vlan 5 type 8021q
RFS7000(config-ext-macl)#
```

The following example marks the tos field to 254 for all IP traffic coming from the source MAC address:

```
RFS7000(config-ext-macl)#mark tos 254 host 00:33:44:55:66:77 any type ip
RFS7000(config-ext-macl)#
```

16.1.7 no

MAC Extended ACL Config Commands

Use this command to negate a command or set defaults.

Syntax

```
no [deny|mark|permit]
```

This command negates all the syntax combinations used in *RFS7000(config-ext-macl)#*, *mark* and *permit* to configure the Extended ACL.

Parameters

no deny	Negates the deny packets rule entry in an MAC extended ACL.
no mark	Negates the mark packets rule entry in an MAC extended ACL.
no permit	Negates the permit packets rule entry in an MAC extended ACL.

Example

```
RFS7000(config-ext-macl)#no mark tos 254 host 00:33:44:55:66:77 any type ip rule-
precedence 50
RFS7000(config-ext-macl)#

RFS7000(config-ext-macl)#no deny any any vlan 5 type 8021q rule-precedence 10
RFS7000(config-ext-macl)#

RFS7000(config-ext-macl)#no permit any any type wisp rule-precedence 50
RFS7000(config-ext-macl)#
```

16.1.8 permit

MAC Extended ACL Config Commands

Use this command to specify packets to forward.

NOTE Use a decimal value representation of Ethertypes to implement permit/deny/mark designations for a packet. Extended MAC ACL's provide hexadecimal values for each listed Ethertype. The switch supports all ethertypes. Use the decimal equvilant of the Ethertype listed in the CLI or for any other type of Ethertype.

A MAC access list (to allow an ARP) is mandatory for both port and WLAN ACL's.

```
permit [<SOURCE-MAC/MASK>|any|host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-MAC/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] {dot1p [<0-7>]|rule-precedence [<1-5000>]|type [<OPTION>]|
  vlan [<1-4095>]}

permit [<SOURCE-MAC/MASK>|any|host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-MAC/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] {dot1p [<0-7>] {rule-precedence <1-5000>|type [<OPTION>]
  rule-precedence <1-5000>}}

permit [<SOURCE-MAC/MASK>|any|host <AA.BB.CC.DD.EE.FF] [<DESTINATION-MAC/MASK>|any|
  host <AA.BB.CC.DD.EE.FF>] {type <OPTION> {rule-precedence <1-5000>}}

permit [<SOURCE-MAC/MASK>|any|host <XX:XX:XX:XX:XX:XX>] [<DESTINATION-MAC/MASK>|any|
  host <XX:XX:XX:XX:XX:XX>] {vlan <1-4095> {rule-precedence <1-5000>|
  type <OPTION> rule-precedence <1-5000>}}
```

Parameters

[<SOURCE-MAC/MASK|any| host <XX:XX:XX:XX:XX:XX>]	Use the `permit` command to forward packets from the specified source and destination network/host. Permits packets from the specified MAC addresses. The source wildcard can be any one of the following: • <SOURCE-MAC/MASK> – The source MAC address and mask in the xx.xx.xx.xx.xx.xx/xx.xx.xx.xx.xx.xx format. • any – Specifies any source host. • host <XX:XX:XX:XX:XX:XX> – Specifies the exact source MAC address to match.
[<DESTINATION-MAC/MASK|any| host <XX:XX:XX:XX:XX:XX>]	Permits packets to the specified destination addresses. The destination wildcard can be any one of the following: • <DESTINATION-MAC/MASK> – The destination MAC address and mask in the xx.xx.xx.xx.xx.xx/xx.xx.xx.xx.xx.xx format. • any – Specifies any source host. • host <XX:XX:XX:XX:XX:XX> – Specifies the exact destination MAC address to match.
dot1p <0-7>	Optional. Specifies the 802.1p priority value to match.
rule-precedence <1-5000>	Optional. Sets the MAC access list entry precedence between 1 - 5000.

type <OPTION>	Optional. Sets the Ethertype value, represented as integer or keywords for well known Ethertypes.The options are: • 8021q – Specifies VLAN Ethertype (0x8100) • <1-65535> – Specifies an Ethernet protocol number • aarp – Specifies *AppleTalk Address Resolution Protocol* (AARP) Ethertype (0x80F3) • appletalk – Specifies APPLETALK Ethertype (0x809B) • arp – Specifies *Address Resolution Protocol* (ARP) Ethertype (0x0806) • ip – Specifies IP Ethertype (0x800) • ipv6 – Specifies IPv6 Ethertype (0x86DD) • ipx – Specifies IPX Ethertype (0x8137) • rarp – Specifies *Reverse Address Resolution Protocol* (RARP) Ethertype (0x8035) • wisp – Specifies WISP Ethertype (0x8783).
vlan <1-4095>	Optional. Specifies the VLAN tag ID to match.

Usage Guidelines

When creating a Port ACL, the switch (by default) does not permit an Ethertype WISP. First create a rule to allow WISP to adopt access ports. Use the following CLI command to adopt access ports:

```
permit any any type wisp
```

NOTE Use the following command to attach a MAC access list to a port on a layer 2 interface:

```
mac access-group <acl number/name> in
```

The permit command in the MAC ACL disallows traffic based on layer 2 (data-link layer) information. The MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, Ethernettype. Common Ethernet types include:

- ARP
- WISP
- IP
- 802.1q

The switch (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access port through an interface, configure an access control list to allow Ethernet WISP.

NOTE To apply an IP based ACL to an interface, a MAC access list entry to allow arp is mandatory. MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

Example

The example below permits WISP based traffic from any source MAC address to any destination MAC address.

```
RFS7000(config-ext-macl)#permit any any type wisp
RFS7000(config-ext-macl)#
```

The example below permits ARP based traffic from any source MAC address to any destination MAC address.

```
RFS7000(config-ext-macl)#permit any any type arp
RFS7000(config-ext-macl)#
```

The example below permits IP based traffic from a particular source MAC address to any destination MAC address.

```
RFS7000(config-ext-macl)#permit host 11:22:33:44:55:66 any type ip
RFS7000(config-ext-macl)#
```

16.1.9 service

MAC Extended ACL Config Commands

Use this command to invoke service commands to troubleshoot or debug `(config-if)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows CLI tree of current mode.

Example

```
RFS7000(config-ext-macl)#service show cliMAC Extended ACL Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-ext-macl)#
```

16.1.10 show

MAC Extended ACL Config Commands

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Usage Guidelines

The `show access-list` command displays the access lists configured for the switch. Provide the access list name or number to view specific ACL details.

Example

```
RFS7000(config-ext-macl)#show ?aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
```

```
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-ext-macl)#
```

17

DHCP Instance

Use the `(config-dhcp)` instance to configure the DHCP server address pool associated with the switch. Use `ip dhcp pool (pool name)` command to reach **`(config-dhcp)`** instance.

17.1 DHCP Config Commands

Table 17.1 summarizes `config-dhcp` commands.

Table 17.1 DHCP Server Config Command Summary

Command	Description	Ref.
address	Configures the DHCP network pool address range.	*page 17-3*
bootfile	Assigns a boot file name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.	*page 17-4*
class	Configures DHCP server class	*page 17-5*
client-identifier	Uses an ASCII string as a client identifier.	*page 17-10*
client-name	Assigns a client name.	*page 17-11*
clrscr	Clears the display screen.	*page 17-12*
ddns	Configures *Dynamic DNS* (DDNS).	*page 17-13*
default-router	Configures the default router's IP address.	*page 17-14*
dns-server	Configures the IP address for the DNS Server.	*page 17-15*
domain-name	Configures the domain name.	*page 17-16*
end	Ends the current mode and moves to the EXEC mode.	*page 17-17*
exit	Ends the current mode and moves to the previous mode.	*page 17-18*
hardware-address	Configures the hardware address using either a dashed or dotted hexadecimal string.	*page 17-19*
help	Describes the interactive help system.	*page 17-20*
host	Configures the IP address for the host.	*page 17-21*
lease	Assigns the lease time for the DHCP IP address.	*page 17-22*

Table 17.1 DHCP Server Config Command Summary

Command	Description	Ref.
netbios-name-server	Configures NetBIOS (WINS) name servers.	*page 17-23*
netbios-node-type	Configures NetBIOS node type.	*page 17-24*
network	Configures a network number and mask for the DHCP Server.	*page 17-25*
next-server	Configures the next server in boot process.	*page 17-26*
no	Negates a command or sets defaults.	*page 17-27*
option	Assigns a name for the DHCP option.	*page 17-28*
service	Displays the service commands for DHCP.	*page 17-29*
show	Displays current running system information.	*page 17-30*
unicast-enable	Enables unicast for DHCP offer and DHCP acknowledgement	*page 17-32*
update	Controls the usage of dynamic DNS.	*page 17-33*

17.1.1 address

DHCP Config Commands

Use this command to specify a range of addresses for DHCP network pool.

Syntax

```
address [range] [<LOW-IP-ADDRESS>] {<HIGH-IP-ADDRESS>}
```

Parameters

range	Configures the address range for the DHCP server.
<LOW-IP-ADDRESS>	Specify the first IP address in the range.
<HIGH-IP-ADDRESS>	Optional. Specify the last IP address in the range. A maximum of 65535 addresses can be configured as the DHCP network pool.

Use the `address` command to specify a range of addresses for the DHCP network pool. The DHCP server assigns an IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address and low IP address is the lower limit for providing the IP address.

Use the `no address (range)` command to remove the DHCP address range.

Example

```
RFS7000(config-dhcp)#address range 2.2.2.2 2.2.2.50
RFS7000(config-dhcp)#


RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.50

RFS7000(config-dhcp)#
```

17.1.2 bootfile

DHCP Config Commands

Use this command to assign a bootfile name for the DHCP configuration on the network pool.

Syntax

```
bootfile <WORD>
```

Parameters

bootfile <WORD>	Indicates the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Usage Guidelines

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients). Only one boot file is allowed per pool.

Use `[no] bootfile` command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command `[no] bootfile` will remove the exisitng command from the pool.

Example

```
RFS7000(config-dhcp)#bootfile bootexample.txt
RFS7000(config-dhcp)#
```

17.1.3 class

DHCP Config Commands

Use this command to associate a DHCP class with a pool. This command is used in Step 4 in the usage guidelines provided below.

The CLI prompt moves to a sub-instance **(config-dhcp-class)** . The configuration mode changes from **(config-dhcp)#class** to **(config-dhcp-class)#**.

Refer to *config-dhcp-class on page 17-7* for `(config-dhcp-class)` command summary.

Syntax

```
class <WORD>
```

Parameters

class <WORD>	Associates a class with a pool and enters DHCP pool class configuration mode.

Usage Guidelines

Follow the steps mentioned below to create a DHCP User Class:

1. Create a DHCP class named **RFS7000DHCPclass**. The switch supports a maximum of 32 DHCP classes.

   ```
   RFS7000(config)#ip dhcp class RFS7000DHCPclass
   RFS7000(config-dhcpclass)#
   ```

2. Create a USER class named **MC800**. The privilege mode changes to `(config-dhcpclass)`. The switch supports a maximum of 8 user classes per DHCP class.

   ```
   RFS7000(config-dhcpclass)#option user-class MC800
   RFS7000(config-dhcpclass)#
   ```

3. Create a Pool named **WID**, using `(config)#` mode.

   ```
   RFS7000(config)#ip dhcp pool WID
   RFS7000(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1, with the pool created in Step 3. The switch supports association of only 8 DHCP classes with a pool.

   ```
   RFS7000(config-dhcp)#class RFS7000DHCPclass
   ```

5. `RFS7000(config-dhcp-class)#`The switch moves to a new mode `(config-dhcp-class)`. Use this mode to add address range to be used for the DHCP class, associated with the pool.

   ```
   RFS7000(config-dhcp-class)#address range 11.22.33.44
   ```

Example

```
RFS7000(config-dhcp)#clas RFS7000DHCPclass
RFS7000(config-dhcp-class)#

RFS7000(config-dhcp-class)#?
DHCP Server Class Config commands:
  address  Configure DHCP Server include range
  clrscr   Clears the display screen
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  no       Negate a command or set its defaults
  service  Service Commands
  show     Show running system information

RFS7000(config-dhcp-class)#
```

17.1.3.1 config-dhcp-class

- *class*

Use `(config-dhcp)# class` to enter the (**`config-dhcp-class`**) instance. Use this instance to set an address range for a DHCP user class in a DHCP server address pool.

Table 17.2 summarizes `config-dhcp-class` commands. ***address***

Table 17.2 Config- dhcp-class Command Summary

Command	Description
Table 17.2 summarizes config-dhcp-class commands. address	Configures a range of IP addresses with this DHCP class.
clrscr	Clears the display screen.
end	Ends current mode and change to EXEC mode.
exit	Ends current mode and moves to the to previous mode.
help	Displays the interactive help system.
no	Negates a command or set its defaults.
service	Displays service commands.
show	Displays running system information.

config-dhcp-class

Use this command to configure a range of IP addresses with this DHCP class.

Syntax

```
address range [<LOW-IP-ADDRESS>] {<HIGH-IP-ADDRESS>}
```

Example

range	Configures a range of addresses with this DHCP class.
<LOW-IP-ADDRESS>	Specify the first IP address in the range
<HIGH-IP-ADDRESS>	Optional. Specify the last IP address in the range.

```
RFS7000(config-dhcp-class)#address range 11.22.33.44
address range 11.22.33.44 RFS7000(config-dhcp-class)#
```

no

config-dhcp-class

Use this command to negate a value or set its default value.

Syntax

```
no address
```

Parameters

Refer to *Table 17.2 summarizes `config-dhcp-class` commands. address on page 17-8* for the parameters negated using the `no` cammand.

```
RFS7000(config-dhcp-class)#no address range all
RFS7000(config-dhcp-class)#
```

17.1.4 client-identifier

DHCP Config Commands

Use this command to assign a name to the client-identifier. A client identifier is used to reserve an IP address for DHCP clients.

Syntax

```
client-identifier <WORD>
```

Parameters

client-identifier <WORD>	Specifies the ASCII string.To prepend a null character, use `\\0` at beginning. A single `\` in the input is ignored.

Example

```
RFS7000(config-dhcp)#client-identifier testid
RFS7000(config-dhcp)#
```

17.1.5 client-name

DHCP Config Commands

Use this command to a add client name for the DHCP clients.

Syntax

```
client-name <WORD>
```

Parameters

client-name <WORD>	Use `client-name` to add a client name. The domain name must not be included.

Example

```
RFS7000(config-dhcp)#client-name testpc
RFS7000(config-dhcp)#
```

17.1.6 clrscr

DHCP Config Commands

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-dhcp)#clrscr
RFS7000(config-dhcp)#
```

17.1.7 ddns

DHCP Config Commands

Use this command to configure dynamic DNS parameters like domain name, enabling multi-user class and IP address of the server.

Syntax

```
ddns [domainname|mutiple-user-class|server|ttl]

ddns [domainname <NAME>|multiple-user-class|server <A.B.C.D> {<A.B.C.D>}|
  ttl <1-864000>]
```

Parameters

domainname <NAME>	Sets domain name used for DDNS updates.
multiple-user-class	Enables multiple user class option.
server <A.B.C.D> {<A.B.C.D>}	Specifies the server to which DDNS updates have been sent. • <A.B.C.D> – The IP address in dotted decimal format. • <A.B.C.D> – Optional. The IP address in dotted decimal format.
ttl <1-864000>	Configures *time to live* (TTL) value used for DDNS updates. • <1-864000> – Specify the TTL value between 1 - 864000 seconds.

Usage Guidelines

A DHCP client cannot perform updates for *resource records* (RRs) A, *text records* (TXTs), and *pointer records* (PTRs). Use `update (dns) (override)` to enable the internal DHCP server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP server can always override the client even if the client is configured to perform the updates.

In the network pool of the DHCP server, FQDN is configured as DDNS domain name. This is used internally in DHCP packets between the DHCP server on the switch and the DNS server.

Example

```
RFS7000(config-dhcp)#ddns domainname TestDomain.com
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#ddns multiple-user-class
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#ddns ttl 1000
RFS7000(config-dhcp)#
```

17.1.8 default-router

DHCP Config Commands

Use this command to configure the default router or gateway IP address for the network pool. To remove the default router list, use the `no default-router` command.

Syntax

```
default-router <ROUTER-IP-ADDRESS>
```

Parameters

default-router <ROUTER-IP-ADDRESS>	Specifies the default router IP address for the network pool. • <ROUTER-IP-ADDRESS> – The router's IP address.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
RFS7000(config-dhcp)#default-router 2.2.2.1
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 default-router 2.2.2.1
 ddns domainname TestDomain.com
 ddns ttl 200
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.50

RFS7000(config-dhcp)#
```

17.1.9 dns-server

DHCP Config Commands

Use this command to configure the DNS server's IP address available to the DHCP clients connected to the pool. Use the `no dns-server` command to remove DNS server list.

Syntax

```
dns-server <A.B.C.D> {<A.B.C.D> <A.B.C.D> .....<A.B.C.D>}
```

Parameters

dns-server <A.B.C.D>	Configures the DNS server's IP address. • <A.B.C.D> – DNS server's IP address.

Usage Guidelines

For DHCP client's, the DNS server's IP address is used to map the host name to IP address. The DHCP client uses the DNS servers IP address based on the order (sequence) configured.

Example

```
RFS7000(config-dhcp)#dns-server 2.2.2.222
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 dns-server 2.2.2.222
 default-router 2.2.2.1
 ddns domainname TestDomain.com
 ddns ttl 200
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.10 domain-name

DHCP Config Commands

Use this command to configure the domain name for the network pool. Use the `no domain-name` command to remove the domain name.

Syntax

```
domain-name <WORD>
```

Parameters

domain-name <WORD>	Configures the domain name for the network pool.

Usage Guidelines

The domain name cannot exceed 256 characters in length.

Example

```
RFS7000(config-dhcp)#domain-name Engineering
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 ddns domainname TestDomain.com
 ddns ttl 200
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.11 end

DHCP Config Commands

Use this command to exit the `config-dhcp` mode and moves to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-dhcp)#end
RFS7000#
```

17.1.12 exit

DHCP Config Commands

Use this command to end the `config-dhcp` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config)#ip dhcp pool TestPool
RFS7000(config-dhcp)#exit
RFS7000(config)#
```

17.1.13 hardware-address

DHCP Config Commands

Use this command to reserve an IP address (manually) based on a DHCP client's hardware address. Use the `no hardware-address` command to remove this from the DHCP pool.

Syntax

```
hardware-address [<XX-XX-XX-XX-XX-XX>|<XX:XX:XX:XX:XX:XX>] {ethernet|token-ring}
```

Parameters

hardware-address [XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX]	Configures the client's hardware address, using one o fthe following formats:. • XX-XX-XX-XX-XX-XX – Dashed-hexadecimal string. • XX:XX:XX:XX:XX:XX – Dotted-hexadecimal string.

Usage Guidelines

This command accepts only hexadecimal values.

Example

```
RFS7000(config-dhcp)#hardware-address 00:01:23:45:32:22
RFS7000(config-dhcp)#
```

17.1.14 help

DHCP Config Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-dhcp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-dhcp)#
```

17.1.15 host

DHCP Config Commands

Use this command to configure a fixed IP address for the host in dotted decimal format. Use the `no host` command to remove the host from the DHCP pool.

Syntax

```
host <IP-ADDRESS>
```

Parameters

host <IP-ADDRESS>	Configures the host's fixed IP address. • <IP-ADDRESS> – IP address in dotted decimal format.

Usage Guidelines

The DHCP host pool (used to manually assign specify IP address based on hardware address/client identifier), configuration must contain a host IP address, client name and hardware address/client identifier.

The host IP address must belong to subnet on the switch. There must be a DHCP network pool corresponding to that host IP address. There is no limit on the number of manual binding's but you can configure only one manual binding per host pool.

Example

```
RFS7000(config-dhcp)#host 2.2.2.111
RFS7000(config-dhcp)#
```

17.1.16 lease

DHCP Config Commands

Use this command to configure a valid lease time for the IP address used by all DHCP clients in the network pool.

Syntax

```
lease [<0-365>|infinite]
lease [<0-365> <0-23> <0-59>]
```

Parameters

lease	Sets the lease time for IP address.

<0-365> <0-23> <0-59>	Sets the lease time in days, hours and minutes.
	• <0-365> – Lease period in days. Days can be made as 0 only when hours and/or mins are greater than 0.
	  • <0-23> – Used with the above to set the hours for the lease period.
	  • <0-59> – Used with the above to set the minutes for the lease period.

infinite	Sets the lease period as infinite

Usage Guidelines

If lease parameter is not configured on the DHCP network pool, the default value is used. The default lease value is 24 hours.

The lease value for DHCP host pool is infinite.

Example

```
RFS7000(config-dhcp)#lease 20 12 30
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 ddns domainname TestDomain.com
 ddns ttl 200
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.17 netbios-name-server

DHCP Config Commands

Use this command to configure the NetBIOS Name server's IP address for the DHCP pool.

Syntax

```
netbios-name-server <IP-ADDRESS>
```

Parameters

netbios-name-server <IP-ADDRESS>	Configures the NetBIOS (WINS) name servers. • <IP-ADDRESS> – NetBIOS name server's IP address.

Example

```
RFS7000(config-dhcp)#netbios-name-server 2.2.2.200
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 netbios-name-server 2.2.2.200
 ddns domainname TestDomain.com
 ddns ttl 200
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.18 netbios-node-type

DHCP Config Commands

Use this command to configure the NetBIOS node type.The node type determines how the NetBIOS Name server resolves NetBIOS names to IP addresses.

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

netbios-node-type [b-node|h-node| m-node|p-node]	NetBIOS (WINS) name servers. • b-node – Broadcast node. • h-node – Hybrid node. • m-node – Mixed node. • p-node – Peer-to-peer node.

Example

```
RFS7000(config-dhcp)#netbios-node-type p-node
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 ddns domainname TestDomain.com
 ddns ttl 200
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.19 network

DHCP Config Commands

Use this command to configure the network pool's IP address. This maps the current DHCP pool with the specified network.

Syntax

Parameters`network [<IP-ADDRESS> <MASK>|<IP-ADDRESS/MASK>]`

network [<IP-ADDRESS> <MASK>| <IP-ADDRESS/MASK>]	Network number and mask. • <IP-ADDRESS> – Network number in dotted decimal format. • <MASK> – Network mask in dotted decimal format. • <IP-ADDRESS/MASK> – Network number and mask.

Usage Guidelines

Ensure a VLAN interface with specific network /subnet exists on the switch before mapping the DHCP pool to a particular network.

Example

```
RFS7000(config-dhcp)#network  2.2.2.0/24
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp con

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 ddns domainname TestDomain.com
 ddns ttl 200
 network 2.2.2.0/24
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.20 next-server

DHCP Config Commands

Use this command to configure the IP address of the Next server in the boot process.

Syntax

```
next-server <IP-ADDRESS>
```

Parameters

next-server <IP-ADDRESS>	Defines the Next server in the boot process. • <IP-ADDRESS> – Server's IP address.

Example

```
RFS7000(config-dhcp)#next-server 2.2.2.22
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 next-server 2.2.2.22
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 ddns domainname TestDomain.com
 ddns ttl 200
 network 2.2.2.0/24
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.21 no

DHCP Config Commands

Use this command to negate a command or set defaults.

Syntax

```
no [address|bootfile|class|client-identifier|client-name|ddns|default-router|
  dns-server|domain-name|hardware-address|host|lease|netbios-name-server|
  netbios-node-type|network|next-server|option|unicast-enable|update]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

The pool has only one bootfile and hence the `<filename >` is not required when using the `[no]` command. To remove a bootfile use `no bootfile` command only.

Example

```
RFS7000(config)#no ip dhcp pool hotpool
RFS7000(config)#

RFS7000(config)#no ip dhcp pool test
RFS7000(config)#

RFS7000(config-dhcp)#no update dns
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#no bootfile
RFS7000(config-dhcp)#
```

17.1.22 option

DHCP Config Commands

Use this command to define the raw DHCP option used in DHCP pools.

Syntax

```
option <OPTION-NAME> [<A.B.C.D>|<WORD>]
```

Parameters

option <OPTION-NAME>	Configures the raw DHCP options.
	• <OPTION-NAME> – Name of the DHCP option.
	  • <A.B.C.D> – IP Value of the DHCP option.
	  • <WORD> – ASCII Value of DHCP option.

Usage Guidelines

Used to define non standard DHCP options option-code (0-254).

Note An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show runnig config` to view the output). Use a double backslash to represent a single backslash

Example

```
RFS7000(config)#ip dhcp option option189 ascii
RFS7000(config)#
```

17.1.23 service

DHCP Config Commands

Use this command to invoke service commands to troubleshoot or debug the `(config-dhcp)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show	Shows running system information.
cli	Shows CLI tree of current mode.

Example

```
RFS7000(config-dhcp)#service show cliDHCP Server Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
 -- MORE --, next page: Space, next line: Enter, quit: Control-CRFS7000(config-dhcp)#
```

17.1.24 show

DHCP Config Commands

Use this command to view current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-dhcp)#show ?

  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information

  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands

  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
```

```
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-dhcp)#show

RFS7000(config-dhcp)#show dhc config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 next-server 2.2.2.22
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 ddns domainname TestDomain.com
 ddns ttl 200
 network 2.2.2.0/24
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#


RFS7000(config)#show dhcp status

DHCP Server is Running on following interfaces

        vlan4

RFS7000(config)#


RFS7000(config)#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------
RFS7000(config)#
```

17.1.25 unicast-enable

DHCP Config Commands

Use this command to enable unicast for DHCP offer and DHCP acknowledgement.

Parameters

None.

Example

```
RFS7000(config-dhcp)#unicast-enable
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 next-server 2.2.2.22
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 unicast-enable
 ddns domainname TestDomain.com
 ddns ttl 200
 network 2.2.2.0/24
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.1.26 update

DHCP Config Commands

Use this command to control the usage of the DDNS service.

Syntax

```
update dns {override}
```

Parameters

update dns {override}	Controls the usage of the DDNS service. • dns – Configures dynamic DNS. • override – Optional. Enables dynamic updates by an onboard DHCP server.

Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR. Use `update (dns) (override)` to enable the internal DHCP Server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can always override the client, even if the client is configured to perform the updates.

In the network pool of DHCP Server, FQDN is configured asa DDNS domain name. This is used internally in DHCP packets between the switch's DHCP Server and the DNS server.

Example

```
RFS7000(config-dhcp)#update dns override
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#show dhcp config

!
ip dhcp pool WID
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 next-server 2.2.2.22
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 unicast-enable
 update dns override
 ddns domainname TestDomain.com
 ddns ttl 200
 network 2.2.2.0/24
 class test
 class RFS7000DHCPclass
!
ip dhcp pool poo1
!
ip dhcp pool pool1
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcp)#
```

17.2 Configuring DHCP Server using CLI

DHCP configuration is conducted by creating pools and mapping them to L3 interfaces (SVI).

A pool can be configured either as a network pool or host pool. A network pool includes ranges. When the network pool is mapped to a L3 interface, DHCP clients requesting IP from the interface get an IP from the included range. A host pool is used to assign static/fixed IP address to DHCP clients.

17.2.1 Creating network pool

```
RFS7000(config)#ip dhcp pool test
RFS7000(config-dhcp)#network 192.168.0.0/24
RFS7000(config-dhcp)#address range 192.168.0.30 192.168.0.60
RFS7000(config-dhcp)#domain-name test.com
RFS7000(config-dhcp)#dns-server 192.168.0.10 192.168.0.11
RFS7000(config-dhcp)#lease 10
RFS7000(config-dhcp)#exit
```

17.2.2 Creating host pool

```
RFS7000(config)#ip dhcp pool hostpool
RFS7000(config-dhcp)#client-name linuxbox
RFS7000(config-dhcp)#host 192.168.0.50
RFS7000(config-dhcp)#hardware 00:a0:f8:6f:6b:88
RFS7000(config-dhcp)#exit
```

17.2.3 Troubleshooting DHCP configuration

DHCP Server configurations come into effect only after rebooting the DHCP Server. Execute the `ip dhcp restart`, at a global level, to restart the DHCP Server. The following steps help setup/troubleshoot DHCP related configuration issues:

1. To change the domain name for a pool from its existing name to `example.com`:

   ```
   RFS7000(config)#ip dhcp pool test
   RFS7000(config-dhcp)#domain-name example.com
   RFS7000(config-dhcp)#exit
   ```

2. Use `service dhcp` to restart the DHCP Server to implement any change made to the configuration. The switch , by default, restarts the DHCP Server after 30 seconds of making a change to the configuration:

   ```
   RFS7000(config)#ip dhcp excluded-address 192.168.0.20 192.168.0.30
   RFS7000(config)#service dhcp
   ```

3. Use the `network` command to map the network pool to interface.

   ```
   network 192.168.0.0/24
   ```

   In the above example, `192.168.0.0/24` represents the L3 interface. When executing this command, no check is performed to verify whether an interface with the specified IP/Netmask exists. A pool can be created and mapped to a non exisitng L3 interface, hence a verification is not required.

   Later (when you add a L3 interface and assign an IP address to it), the DHCP Server gets enabled/started on the interface. If you have a pool for `192.168.0.0/24`, but the L3 interface is `192.168.0.0/16`, DHCP wont be enabled on 192.168.0.0/16, as it is different from `192.168.0.0/24`.

4. A network pool without any include range is as good as not having a pool at all. Add an include range using the `address range` CLI command

   ```
   address range 192.168.0.30 192.168.0.30
   ```

5. To work properly, a host pool should have the following 3 items configured:

   - client-name (CLI is `client-name <name>`)
   - fixed-address (CLI is `host <ip>`)
   - hardware-address/client-identifier

     CLI for hardware address is `hardware-address <addr>`

     CLI for client-identifier is `client-identifier <id>`

   If using `client-identifier` instead of `hardware-address`, the DHCP client sends the client-identifier when it requests for IP address.

6. A host pool should have its corresponding network pool configured, otherwise the host pool is useless. The fixed IP address configured in the host pool must be in the subnet of the corresponding network pool.
7. Use the global configuration mode `service dhcp` to enable/disable the DHCP Server. This enables/disables the DHCP Server on all interfaces.
8. If you create a pool and map it to interface, it automatically gets enabled, provided DHCP is enabled at the global level. Use the `no network` command to disable DHCP on a per pool/interface basis.
9. To add a newly created pool to the network pool, use one of the following:

   - `network ( Eg network 192.168.0.0/24 )`
   - `address range ( Eg address range 192.168.0.30 192.168.0.50 )`

10. To add a newly created pool to host pool, use one of the following:

- `host ( Eg host 192.168.0.1 )`
- `client-name ( Eg client-name "kaveri" )`
- `client-identifier ( Eg client-identifier "aabb:ccdd" )`
- `hardware-address ( Eg hardware-address aa:bb:cc:dd:ee:ff )`

11. A pool can be configured as the host pool or network pool, but not both.
12. A host pool can have either `client-identifier` or `hardware-address` configured, but not both.
13. An excluded address range has higher precedence then an included address range. If a range is part of both an excluded and included address range, it will be excluded.
14. DHCP options are first defined at the global level, using `ip dhcp option <name> <code> <type>`. The value for these options are associated using the `option` which is under DHCP pool context.

18

DHCP Class Instance

Use **(config)#ip dhcp class <class name>** to enter **(config-dhcpclass)** instance. Use this instance to configure the DHCP user class. The switch supports a maximum of 8 user classes per DHCP class.

Also refer *ip on page 5-35* and *DHCP Instance on page 17-1* for other DHCP related configurations.

18.1 DHCP Server Class Config Commands

Table 18.1 summarizes DHCP server class config commands.

Table 18.1 DHCP server class config commands

Command	Description	Ref.
clrscr	Clears the display screen.	*page 18-2*
end	Ends the current mode and moves to the EXEC mode.	*page 18-3*
exit	Ends the current mode and moves to the previous mode.	*page 18-4*
help	Displays the interactive help system.	*page 18-5*
multiple-user-class	Enables multiple user class option.	*page 18-6*
no	Negates a command or set its defaults.	*page 18-7*
option	Configures DHCP Server options.	*page 18-8*
service	Displays service Commands.	*page 18-9*
show	Displays running system information.	*page 18-10*

18.1.1 clrscr

DHCP Server Class Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-dhcpclass)#clrscr
RFS7000(config-dhcpclass)#
```

18.1.2 end

DHCP Server Class Config Commands

Use this command to end and exit from the `config-dhcpclass` mode and change to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-dhcpclass)#end
RFS7000#
```

18.1.3 exit

DHCP Server Class Config Commands

Use this command to end the `config-dhcpclass` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-dhcpclass)#exit
RFS7000(config)#
```

18.1.4 help

DHCP Server Class Config Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-dhcpclass)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-dhcpclass)#
```

18.1.5 multiple-user-class

DHCP Server Class Config Commands

Use this command to enable the multiple user class option. This specifies the client (MU) sends multiple user classes.

Syntax

```
multiple-user-class
```

Parameters

None

Example

```
RFS7000(config-dhcpclass)#multiple-user-class
RFS7000(config-dhcpclass)#
```

18.1.6 no

DHCP Server Class Config Commands

Use this command to negate a command or set its defaults.

Syntax

```
no [multiple-user-class|option]
```

Parameters

multiple-user-class	Disables the multiple user class option.
option	Removes the DHCP server options.

Example

```
RFS7000(config-dhcpclass)#no multiple-user-class
RFS7000(config-dhcpclass)#
```

18.1.7 option

DHCP Server Class Config Commands

Use this command to specify a value for DHCP user class options. This command is used in *Step 2* in the usage guidelines provided below.

Syntax

```
option [user-class] [user class name]
```

Parameters

user-class [user classname]	Creates a DHCP server user-class option.

Usage Guidelines

Follow the steps below to create a DHCP User Class:

1. Create a DHCP class named **`RFS7000DHCPclass`**. RFS7000 supports a maximum of 8 DHCP classes.

   ```
   RFS7000(config)#ip dhcp class RFS7000DHCPclass
   RFS7000(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The privilege mode changes to `(config-dhcpclass)`. RFS7000 supports a maximum of 8 Users classes per DHCP class.

   ```
   RFS7000(config-dhcpclass)#option user-class MC800
   RFS7000(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using `(config)#` mode.

   ```
   RFS7000(config)#ip dhcp pool WID
   RFS7000(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. RFS7000 supports association of only 8 CDHCP classes with a pool.

   ```
   RFS7000(config-dhcp)#class RFS7000DHCPclass
   RFS7000(config-dhcp-class)#
   ```

5. The switch moves to a new mode (config-dhcp-class). Use this mode to add a address range used for the DHCP class associated with the pool.

   ```
   RFS7000(config-dhcp-class)#address range 11.22.33.44
   ```

Example

```
RFS7000(config-dhcpclass)#option user-class MC800
RFS7000(config-dhcpclass)#
```

18.1.8 service

DHCP Server Class Config Commands

Use this command to invoke service commands to troubleshoot or debug (config-if) instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show (cli)	Displays the CLI tree of current mode.

Example

```
RFS7000(config-dhcpclass)#service show cli
DHCP Server Class Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-dhcpclass)#
```

18.1.9 show

DHCP Server Class Config Commands

Use this command to view the current system information.

Syntax

```
show <parameters>

show dhcp [config|status]
show ip dhcp [binding|class|pool|sharednetwork]
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
RFS7000(config-dhcpclass)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
```

```
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-dhcpclass)#show

RFS7000(config-dhcpclass)#show ip dhcp binding

IP               MAC/Client-Id       Expiry Time
--               -------------       -----------
10.10.10.109     00:a0:f8:bf:8a:4b  Mon Sep 17 12:32:53 2007
10.10.10.110     00:0e:9b:98:f9:34  Mon Sep 17 13:34:31 2007
RFS7000(config-dhcpclass)#

RFS7000(config-dhcpclass)#show ip dhcp class
!
ip dhcp class test
 option user-class test
!
ip dhcp class RFS7000DHCPclass
 option user-class MC800
 multiple-user-class

RFS7000(config-dhcpclass)#

RFS7000(config-dhcpclass)#show ip dhcp pool
DHCP pool-id: WID
 Pool Utilization: Available=0, Used=0, Util=0%
 lease 20 12 30
 domain-name Engineering
 dns-server 2.2.2.222
 default-router 2.2.2.1
 next-server 2.2.2.22
 netbios-name-server 2.2.2.200
 netbios-node-type p-node
 unicast-enable
 update dns override
 ddns domainname TestDomain.com
 ddns ttl 200
 network 2.2.2.0/24
 class test
 class RFS7000DHCPclass
DHCP pool-id: poo1
 Pool Utilization: Available=0, Used=0, Util=0%
DHCP pool-id: test
 Pool Utilization: Available=0, Used=0, Util=0%
DHCP pool-id: pool1
 Pool Utilization: Available=99, Used=0, Util=0%
 address range 2.2.2.2 2.2.2.100

RFS7000(config-dhcpclass)#
```

19

RADIUS Server Instance

The **radius-server local** command moves to the RADIUS server mode. The local (Onboard) RADIUS server configuration commands are listed under this mode. Use the **(config-radsrv)** instance to configure local RADIUS server parameters.

19.1 RADIUS Configuration Commands

Table 19.1 summarizes the RADIUS Config commands.

Table 19.1 RADIUS Config Command Summary

Command	Description	Ref.
authentication	RADIUS authentication.	*page 19-3*
ca	Configures ca certificate parameters.	*page 19-4*
clrscr	Clears the display screen.	*page 19-5*
crl-check	Certificate Revocation List (CRL) check.	*page 19-6*
end	Ends the current mode and moves to the EXEC mode.	*page 19-7*
exit	Ends the current mode and moves to the previous mode.	*page 19-8*
group	Configures RADIUS user group parameters. **Note:** Creates another sub-instance called **config-radsrv -group** with its own command summary.	*page 19-9*
help	Displays the interactive help system.	*page 19-27*
ldap-group-verification	Enables/disables LDAP group verification.	*page 19-28*
ldap-server	LDAP server parameters.	*page 19-29*
nas	RADIUS client.	*page 19-31*
no	Negates a command or set its defaults.	*page 19-32*
proxy	RADIUS proxy server.	*page 19-33*
rad-user	RADIUS user configuration.	*page 19-34*

Table 19.1 RADIUS Config Command Summary

Command	Description	Ref.
server	Configures server certificate parameters.	*page 19-36*
service	Service commands.	*page 19-37*
show	Shows running system information.	*page 19-38*

19.1.1 authentication

RADIUS Configuration Commands

Use this command to configure an authentication scheme used with the RADIUS server.

Syntax

```
authentication [data-source|eap-auth-type]

authentication data-source [ldap|local]

authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|
  ttls-mschapv2|ttls-pap]
```

Parameters

data-source [ldap|local]	Configures one of the following RADIUS data sources for user authentication: • ldap – The remote *Lightweight Directory Access Protocol* (LDAP) server's database. • local – The wireless controller's local user database.
eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]	Configures RADIUS *Extensible Authentication Protocol* (EAP) and default authentication type used with this RADIUS policy. • all – Enables both TTLS and PEAP settings. • peap-gtc – Configures EAP type PEAP with default auth type GTC. • peap-mschapv2 – Configures EAP type PEAP with default auth type MSCHAPV2. • tls – Uses TLS as the EAP type.. • ttls-md5 – Configures EAP type TTLS with default auth type MD5. • ttls-mschapv2 – Configures EAP type TTLS with default auth type MSCHAPV2. • ttls-pap – Configures EAP type TTLS with default auth type PAP.

Usage Guidelines

Set `eap-auth-type` to `all` to service any RADIUS request received from a mobile unit. Setting `eap-auth-type` to `peap-gtc/ peap-mschapv2` ensures `peap-gtc/peap-mschapv2` service only.

Similarly, set `eap-auth-type` to `ttls-md5/ttls-mschapv2/ttls-pap` to service all TTLS based authentication RADIUS requests from the mobile unit.

Setting `eap-auth-type` to `tls` ensures only tls authentications are serviced.

Example

```
RFS7000(config-radsrv)#authentication eap-auth-type peap-mschapv2
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#authentication data-source ldap
RFS7000(config-radsrv)#
```

19.1.2 ca

RADIUS Configuration Commands

Use this command to configure *Certificate Authority* (CA) parameters.

Syntax

```
ca trust-point <TRUSTPOINT-NAME>
```

Parameters

trust-point <TRUSTPOINT-NAME>	Trustpoint configuration. • <TRUSTPOINT-NAME> – Specify an existing trustpoint name.

Usage Guidelines

Configure the trustpoint used by the local RADIUS server. Use the **`crypto pki trustpoint`** command to create the **`trustpoint`** before using it.

The default trustpoint in use is – `default-trustpoint.`

Example

In the example below, the trustpoint (`tp1)` already has a certificate associated with it.

```
RFS7000(config)#radius-server local
RFS7000(config-radsrv)#ca trust-point tp1
RFS7000(config-radsrv)#
```

19.1.3 clrscr

RADIUS Configuration Commands

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#clrscr
RFS7000(config-radsrv)#
```

19.1.4 crl-check

RADIUS Configuration Commands

Use this command to enable a *Certificate Revocation List* (CRL) check. To enable the CRL check, ensure the `crl list` is loaded using the **`crypto pki import <trustpoint-name> crl`** command.

Syntax

```
crl-check enable
```

Parameters

enable	Enables CRL check.

Usage Guidelines

A CRL that is updated with a trustpoint contains index numbers of all the revoked certificates. tls authentication type uses certificate for authentication and the CRL checks for any revoked certificate used for tls authentication.

Example

```
RFS7000(config-radsrv)#crl-check enable
RFS7000(config-radsrv)#
```

19.1.5 end

RADIUS Configuration Commands

Use this command to exit from the `config-radsrv` mode and move to the PRIV EXEC mode. The prompt now changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#end
RFS7000#
```

19.1.6 exit

RADIUS Configuration Commands

Use this command to exit the `config-radsrv` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#exit
RFS7000(config)#
```

19.1.7 group

RADIUS Configuration Commands

Use this command to configure RADIUS user groups. The CLI moves to a sub-instance **config-radsrv-group**, to create a new group.

The prompt changes from **RFS7000(config-radsrv)#** to **RFS7000(config-radsrv-group)#.**

Table 19.2 summarizes the RADIUS User Group commands within the **(config-radsrv-group)** sub-instance.

Table 19.2 RADIUS User Group Configuration Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	*page 19-10*
end	Ends the current mode and changes to the EXEC mode.	*page 19-11*
exit	Ends the current mode and moves to the previous mode.	*page 19-12*
group	Configures RADIUS user group parameters.	*page 19-13*
guest-group	Guest group configuration.	*page 19-14*
help	Describes the interactive help system.	*page 19-15*
no	Negates a command or set its defaults.	*page 19-16*
policy	RADIUS group access policy configuration.	*page 19-18*
rad-user	Adds a RADIUS user to a group.	*page 19-20*
rate-limit	Sets rate limit for group	*page 19-21*
service	Service Commands.	*page 19-22*
show	Shows running system information.	*page 19-23*

19.1.7.1 clrscr

group

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#clrscr
RFS7000(config-radsrv-group)#
```

19.1.7.2 end

group

Use this command to exit the `config-radsrv-group` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#end
RFS7000#
```

19.1.7.3 exit

group

Use this command to exit the `config-radsrv-group` mode and move to the previous mode `(config-radsrv)`). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#exit
RFS7000(config-radsrv)#
```

19.1.7.4 group

group

Use this command to configure RADIUS user groups. This command creates a group within an existing RADIUS group.

Syntax

```
group <GROUP-NAME>
```

Parameters

<GROUP-NAME>	Specify the RADIUS group name (cannot exceed 32 characters in length).

Example

```
RFS7000(config-radsrv)#group TestGroup
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#show radius group

Group Details
_____________
Group Name        : test
Vlan              : Not configured
Group Policy
-----------
        Wlan's Allowed : None
        Day Of Access  : All
        Start Time     : 0000  ( in hhmm )
        End Time       : 2359  ( in hhmm )
        wired-to-wireless Limit   : unlimited
        wireless-to-wired Limit   : unlimited


Group Name        : TestGroup
Vlan              : Not configured
Guest-Group       : Enabled
Group Policy
-----------
        Wlan's Allowed : None
        Day Of Access  : All
        Start Time     : 0000  ( in hhmm )
        End Time       : 2359  ( in hhmm )
        wired-to-wireless Limit   : unlimited
        wireless-to-wired Limit   : unlimited


Group Name        : RadiusGrp1
Vlan              : Not configured
Group Policy
-----------
        Wlan's Allowed : None
        Day Of Access  : All
        Start Time     : 0000  ( in hhmm )
        End Time       : 2359  ( in hhmm )
        wired-to-wireless Limit   : unlimited
        wireless-to-wired Limit   : unlimited

RFS7000(config-radsrv-group)#
```

19.1.7.5 guest-group

group

Use this command to manage a guest user linked with a hotspot. Additionally, create a guest-user and associate it with a guest-group. The guest-user and the policies of the guest-group are used for hotspot authentication.

Syntax

```
guest-group
```

Parameters

enable	Enables this group as a guest group.

Usage Guidelines

Use this command to create a guest group. The guest user created using the `rad-user` command must only be part of the guest group.

Guest user groups cannot be made manager groups with unique access and role permissions.

Example

```
RFS7000(config-radsrv-group)#guest-group enable
RFS7000(config-radsrv-group)#
```

19.1.7.6 help

group

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-radsrv-group)#
```

19.1.7.7 no

group

Use this command to negate a command or set defaults.

Syntax

```
no [policy|rad-user|rate-limit]
no policy [day|time|vlan|wlan [<1-256> {<1-256>}|all]]
no rad-user [<USER-NAME>|all]
no rate-limit [WIRED-TO-WIRELESS|WIRELESS-TO-WIRED]
```

Parameters

no (policy)	
policy	Resets the RADIUS group access policy configuration.
day	Resets the access policy (daysof permitted access) for this group.
time	Resets the group's hourly access permissions.
vlan	Resets the VLAN ID for this group.
wlan [<1-256> {1-256}| all]	Resets WLAN access policy for this group. • <1-256> – Removes access for the specified range of WLANs. • all – Removes access for all WLANs.
no (rad-user)	
rad-user	Removes users from this group.
<USER-NAME>	Removes a specified user from this group. Specify the user name to remove.
all	Removes all users from this group.
no (rate-limit)	
rate-limit	Resets rate-limits for the group.
wired-to-wireless	Resets rate limits in the up link direction - from wireless client to network
wireless-to-wired	Resets rate limits in the down link direction - from network to wireless client

Example

```
RFS7000(config-radsrv-group)#no policy day
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no policy time
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no policy vlan
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no policy wlan 2 5
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no rad-user all
RFS7000(config-radsrv-group)#
```

19.1.7.8 policy

group

Use this command to configure authorization policies for a particular group, like day/time of access, WLAN's allowed and to set a user based VLAN.

NOTE User based VLAN is effective only if dynamic VLAN authorization is enabled on the WLAN.

Syntax

```
policy [day|time|vlan|wlan]
policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we)}
ploicy time [start|end] <0-23> <0-59>
policy vlan <1-4094>
policy wlan <1-256>
```

Parameters

day	Configures the days on which this group has access The options are: • all – All days (from Sunday to Saturday). • fr – Friday • mo – Monday • sa – Saturday • su – Sunday • th – Thursday • tu – Tuesday • we – Wednesday • weekdays – Allows access only on week days (Mo-Fr).

time	Configures the time when this group has access. The options are:
	• start – Sets the start time.
	  • <0-23> – hour (hh) limit.
	  • <0-59> – mins (mm) limit.
	• end –Sets the end time (must be greater than the start time).
	  • <0-23> – hour (hh) limit.
	  • <0-59> – mins (mm) limit.

vlan	Sets the VLAN ID for this group. • <1-4094> – Specify the VLAN ID between 1 - 4094.
wlan	Configure WLAN access policy for this group. • <1-256> – Specify the WLAN index.

Example

```
RFS7000(config-radsrv-group)#policy day weekdays
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#policy time start 12 12 end 22 22
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#policy vlan 20
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#policy wlan 20 21 22 23
RFS7000(config-radsrv-group)#
```

19.1.7.9 rad-user

group

Use this command to add an existing RADIUS user to this group. If the RADIUS user is not available in the Onboard RADIUS server's database, create a new RADIUS user using `rad-user` command from **`(config-radsrv)`** mode. For more details check *19.1.14 rad-user* on page 34.

Syntax

```
rad-user <USER-NAME>
```

Parameters

<USER-NAME>	Specify an existing RADIUS user name.

Example

```
RFS7000(config-radsrv)#rad-user user1 password user1
RFS7000(config-radsrv)#group group1
RFS7000(config-radsrv-group)#rad-user user1
RFS7000(config-radsrv-group)#
```

19.1.7.10 rate-limit

group

Use this command to set rate limit for this group.

Syntax

```
rate-limit [wired-to-wireless|wireless-to-wired] <100-1000000>
```

Parameters

wired-to-wireless	Configures the rate-limit in the down link direction - from network to wireless client.
wireless-to-wired	Configures the rate-limit in the up link direction - from wireless client to network.
<100-1000000>	Rate in the range of <100-1000000> kbps

Example

```
RFS7000(config-radsrv-group)#rate-limit wired-to-wireless 100
RFS7000(config-radsrv-group)#
```

19.1.7.11 service

group

Use this command to invoke RADIUS service commands. This command is used to enable the RADIUS Server. A service RADIUS restart is executed only from the **config** mode.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows running system information.

Example

```
RFS7000(config-radsrv-group)#service show cliRadius user group configuration mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
    +-dhcp
 -- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-radsrv-group)#
```

19.1.7.12 show

group

Use this command to view the current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command. For additional information, refer to *radius* and *show*.

Example

```
RFS7000(config-radsrv-group)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information

  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands


  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
```

```
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-radsrv-group)#show

RFS7000(config)#show radius trust-point

Trust-point Configured For Radius
_____________________________________
        Server Trust-point : tp1
        CA Trust-point     : default-trustpoint


RFS7000(config)#show radius configuration

Radius Server Configuration
---------------------------
         Server Status : enabled
         Data Source   : local

RFS7000(config)#
```

19.1.7.13 Example–Creating a Group

The use of the **(config-radsrv-group)** sub-instance is explained below:

1. Create a group called **Sales** in the local RADIUS Server database.
   RFS7000(config-radsrv)#group sales
2. Check RADIUS user group configuration commands.

```
RFS7000(config-radsrv-group)#?
Radius user group configuration commands:
  clrscr       Clears the display screen
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  group        Configure radius user group paramaters
  guest-group  Guest group configuration
  help         Description of the interactive help system
  no           Negate a command or set its defaults
  policy       Radius group access policy configuration
  rad-user     Add Radius user to this group
  rate-limit    Set rate limit for group
  service      Service Commands
  show        Show running system information
```

3. Use the **policy** command to configure group policies for the group created in Step 1.

```
RFS7000(config-radsrv-group)#policy ?
day   Day of access policy configuration
time  Configure time of access policy for this group
vlan  VLAN id for this group
wlan  Configure wlan access policy for this group
RFS7000(config-radsrv-group)#policy day weekdays
RFS7000(config-radsrv-group)#policy time start 12 30 end 15 30
```

4. Use the **policy vlan** command to assign VLAN ID of 10 to Sales group.

```
RFS7000(config-radsrv-group)#policy vlan 10
```

5. Use the **policy wlan** command to allow only authorised users to access this group's wlan.

```
RFS7000(config-radsrv-group)#policy wlan 1 2 5
```

6. Use `(config-radsrv)#rad-user` to create a user called **testuser** and add it to the **Sales** group.

```
RFS7000(config-radsrv)#rad-user testuser password testpassword group sales
Nov 08 17:41:55 2011: RADCONF: Adding user "testuser" into local database
Nov 08 17:41:55 2011: RADCONF: User "testuser" is added to group "sales"
```

7. Use **(config-radsrv)#nas** to add a NAS entry.

```
RFS7000(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

RFS7000(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

RFS7000(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
```

```
LINE  The secret(client shared secret), upto 32 characters
RFS7000(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

8. Use **`(config-radsrv)#proxy`** to add a realm name.

```
RFS7000(config-radsrv)#proxy realm mydomain.com server 10.10.1.10 port 1812 secret 0
testing
```

9. Save the changes and restart the RADIUS service.

```
RFS7000(config-radsrv)#service radius restart
Nov 08 17:48:04 2011: %PM-5-PROCSTOP: Process "radiusd" has been stopped
Nov 08 17:48:05 2011: RADCONF: radius config files generated successfully
RFS7000(config-radsrv)#Nov 08 17:48:05 2011: %DAEMON-6-INFO: radiusd[8830]: Ready to
process requests.
```

19.1.8 help

RADIUS Configuration Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#help?
  help  Description of the interactive help system

RFS7000(config-radsrv)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-radsrv)#
```

19.1.9 ldap-group-verification

RADIUS Configuration Commands

Use this command to enable/disable LDAP group verification feature.

Syntax

```
ldap-group-verification [enable|disable]
```

Parameters

enable	Enables LDAP group verification (this is the default setting)
disable	Disables LDAP group verification

Example

```
RFS7000(config-radsrv)#ldap-group-verification enable
RFS7000(config-radsrv)#
```

19.1.10 ldap-server

RADIUS Configuration Commands

Use this command to configure the external LDAP server parameters. It uses the existing external database in form of an active directory with the onboard RADIUS server instead of a local database on the switch.

Syntax

```
ldap-server [primary|secondary]

ldap-server [primary|secondary] [host <LDAP-IP-ADDRESS>] [port <389-389>]
  [login <LOGIN-NAME>] [bind-dn <BIND-NAME>] [base-dn <BASE-NAME>]
  [passwd [0 <WORD>|2 <WORD>|<WORD>]] [passwd-attr <LDAP-SERVER-ATTR>]
  [group-attr <GROUP-ATTR>] [group-filter <GROUP-FILTER>] [group-membership <GROUP>]
  {net-timeout <1-10>}
```

Parameters

primary	Configures the primary LDAP server.
secondary	Configures the secondary LDAP server.
host <LDAP-IP-ADDRESS>	Configures the host LDAP server's IP address. • <LDAP-IP-ADDRESS> – Specify the external LDAP server's IP address.
port <389-389>	Configures the physical port number used by the wireless controller's RADIUS server to connect to the external LDAP server. Enter the TCP/IP port number for the LDAP server acting as the data source.
login <LOGIN-NAME>	Configures the login name used to access the remote LDAP server resource. Provide a unique login name (should not exceed 127 characters in length) Use the following as the login: `(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})`
bind-dn <BIND-NAME>	Configures the distinguished name used to bind with the LDAP server.
base-dn <BASE-NAME>	Configures a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.
passwd [0 <WORD>| 2 <WORD>| <WORD>]	Configures a valid password for the LDAP server. The options are: • 0 <WORD> – Password is specified UNENCRYPTED. • 2 <WORD> – Password is specified encrypted with password-encryption secret. • <WORD> – The LDAP server bind password of size 31.
passwd-attr <LDAP-SERVER-ATTR>	Configures the password attribute used by the LDAP server for authentication. The password attribute is of size 63.
group-attr <GROUP-ATTR>	Configures the group attribute used by the LDAP server. The group attribute is of size 32. **Note:** An attribute can be a group name, group ID, password or group membership name.

group-filter <GROUP-FILTER>	Configures the group filters used by the LDAP server. The group filter is of size 255. **Note:** The group filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.
group-membership <GROUP>	Specifies the group member attribute sent to the LDAP server when authenticating users. The group member attribute is of size 63.
net-timeout <1-10>	Optional. Configures a timeout value. This is the interval the wireless controller's RADIUS server uses as a wait period for a response from the target primary or secondary LDAP server resource. The default is 10 seconds. • <1-10> – Specify a net time out between 1 - 10.

Usage Guidelines

Use the login filter and group filter values, described in the example on the following page, for all LDAP configuration scenarios.

Use `passwd` parameter to enter the password for active directory user mentioned in bind -dn. This will be used for initial login to the active directory.

The `passwd-attr` and `group-membership` is retained as described in the example.

Example

```
RFS7000(config)#ldap-server primary host 192.192.1.88 port 389 login
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}}) bin
d-dn cn=admin,ou=wid,dc=symbolTech,dc=local base-dn ou=wid,dc=symbolTech,dc=local passwd
SYMBOL@123 passwd-attr UserPassword
group-attr cn group-filter (|(&(objectClass=group)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{L
dap-UserDn}))) group-membership radiusGroupName net-timeout 1
RFS7000(config)#
```

19.1.11 nas

RADIUS Configuration Commands

Use this command to configure the RADIUS clients.

Syntax

```
nas [<A.B.C.D/M>] key [0 <LINE>|2 <LINE>|<LINE>]
```

Parameters

<A.B.C.D/M>	Configures the RADIUS client's IP address in the A.B.C.D/M format.
key [0 <LINE>| 2 <LINE>|<LINE>]	RADIUS Client shared key. • 0 <LINE> – Password is specified UNENCRYPTED. • 2 <LINE> – Password is encrypted with password-encryption secret. • <LINE> – The secret (client shared secret), up to 64 characters.

Usage Guidelines

Configure the IP address range in *Network Access Service* (NAS) to service RADIUS access request from clients within the range mentioned. Only 25 NAS entries can be configured on a RFS7000.

Example

```
RFS7000(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

RFS7000(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

RFS7000(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

RFS7000(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

19.1.12 no

RADIUS Configuration Commands

Use this command to negate a command or set its defaults.

Syntax

```
no [authentication|ca|crl-check|group|ldap-server|nas|proxy|rad-user|server]
```

Parameters

no authentication	Removes RADIUS authentication.
ca	Removes ca certificate parameters.
crl-check	Disables CRL check.
group	Removes local RADIUS server group configuration.
ldap-server	Removes LDAP server parameters.
nas	Removes the configured RADIUS clients.
proxy	Removes the RADIUS proxy server.
rad-user	Removes configured RADIUS users.
server	Removes configured server certificate parameters.

Example

```
RFS7000(config-radsrv)#no authentication data-source
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#no ca trust-point
RFS7000(config-radsrv)#
```

19.1.13 proxy

RADIUS Configuration Commands

Use this command to configure a proxy RADIUS server based on the realm/suffix. A user's request is forwarded to the proxy RADIUS server if it cannot be authenticated by the local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects it. If the request is accepted, the proxy server returns configuration information specifying the type of connection service required to authenticate the user.

Syntax

```
proxy [realm|retry-count|retry-delay]
proxy [relam <WORD>] [server <IP-Address>] [secret [0 <WORD>|2 <WORD>|<WORD>]]
```

Parameters

proxy (realm)	
realm <WORD>	Configures the realm name (is a string of up to 50 characters).
server <IP-ADDRESS>	Sets the proxy server's IP address.
secret [0 <WORD>| 2 <WORD>|<WORD>]	Configures the server's shared secret. • 0 <WORD> – Password is specified UNENCRYPTED. • 2 <WORD> – Password is encrypted with password-encryption secret. • <WORD> – The proxy server shared secret up to 32 characters.
proxy (retry-count)	
retry-count <3-6>	Configures the proxy server's retry count value. This value defines the number of retries sent to the proxy server before giving up the request (the default is 3)
proxy (retry-delay)	
retry-delay <5-10>	Configures the proxy server's retry delay time (in seconds). This is the interval the wireless controller's RADIUS server waits before making an additional connection attempt (the default is 5 seconds)

Usage Guidelines

Only five RADIUS proxy server's can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times the switch transmits each RADIUS request to the server before giving up. The timeout value defines the duration for which the switch waits for a reply to a RADIUS request before retransmitting the request.

Example

```
RFS7000(config-radsrv)#proxy realm Test server 10.10.10.1 secret "Very Very Secret !!!"
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#proxy retry-count 5
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#proxy retry-delay 8
RFS7000(config-radsrv)#
```

19.1.14 rad-user

RADIUS Configuration Commands

Use this command to configure RADIUS user parameters.

Syntax

```
rad-user <WORD> [access|password|privilege]

rad-user <WORD> access [console {ssh}|ssh {console}]

rad-user <WORD> password [0 <WORD>|2 <WORD>|<WORD>] {group <GROUP-NAME>}
  {guest [expiry-time <HH:MM>] [expiry-date <MM:DD:YYYY>]}
  {start-time <HH:MM> start-date <MM:DD:YYYY>} {access-duration <30-35791390>}

rad-user <WORD> privilege [crypto-officer|monitor|superuser|superadmin|webadmin]
```

Parameters

<WORD>	Enter a user name up to 64 characters in length.
rad-user <word> (access)	
access [console|ssh]	Sets management user access mode. • console – Only allowed from console. • ssh – Only allowed from ssh.
rad-user <word> (password)	

password [0 <WORD>| 2 <WORD>|<WORD>]	Configures the RADIUS user's password.
	• 0 <WORD> – Password is specified as UNENCRYPTED.
	• 2 <WORD> – Password is encrypted with a password-encryption secret.
	• <WORD> – Enter password up to 21 characters in length.
	  • group <GROUP-NAME> – Optional. Specifies the RADIUS server group configuration.
	  • guest – Optional. Enables guest user access.
	  • expiry-time <HH:MM> – Sets the expiry time for the guest user.
	  • expiry-date <MM:DD:YYYY> – Sets the expiry date for the guest user.
	  • start-time <HH:MM> – Sets the starting time for the guest user.
	  • start-date <MM:DD:YYYY> – Sets the starting date for the guest user.
	  • access-duration <30-35791390> – Optional. Sets the user access duration between 30 - 35791390 minutes.

rad-user <word> (privilege)	
privilege [cryptp-officer|monitor|superuser|sysadmin|webadmin]	Sets management user access privilege. The options are: • crypto-officer – Crypto officer and Network (wired/wireless) admin access • monitor – Monitor (read-only) access. • superuser – Superuser (root) access. • sysadmin – System (general system configuration) admin access. • webadmin – Web auth (hotspot) user admin access.

Usage Guidelines

Use `group,guest, expiry-time expiry-date,start-time` and `start-date` parameters to create a RADIUS guest user.

The RADIUS user group specified while creating a guest user must be a *guest-group*.

Example

```
RFS7000(config-radsrv)#rad-user TestRadUser password "I SPY U"
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#rad-user guest1 password 0 password1 group guest-group
guest expiry-time 12:12 expiry-date 05:12:2012 start-time 12:12 start-date
05:11:2012RFS7000(config-radsrv)#
```

19.1.15 server

RADIUS Configuration Commands

Use this command to configure the server certificate parameters used by the RADIUS server. The server certificate is a part of a trustpoint created *crypto on page 5-23*.

Syntax

```
server trust-point <TRUSTPOINT-NAME>
```

Parameters

trust-point <TRUSTPOINT-NAME>	Trustpoint configuration. • <TRUSTPOINT-NAME> – Specify an existing trustpoint name.

Usage Guidelines

Create a trustpoint using `(crypto-pki-trustpoint)`. Server certificate is created under the trustpoint using crypto-pki commands. Refer to *crypto on page 5-23* for more details.

Example

```
RFS7000(config-radsrv)#server trust-point TestTP
RFS7000(config-radsrv)#
```

19.1.16 service

RADIUS Configuration Commands

Use this command to invoke service commands to troubleshoot or debug `(config-radsrv)` instance configurations. This command is also used to enable the RADIUS Server.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows running system information.

Example

```
RFS7000(config-radsrv)#service show cliRadius Configuration mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
    +-access-list [show ip access-list]
    +-arp [show ip arp]
    +-ddns
      +-binding [show ip ddns binding]
    +-dhcp
      +-binding [show ip dhcp binding]
        +-manual [show ip dhcp binding manual]
      +-class [show ip dhcp class ( WORD | )]
        +-WORD [show ip dhcp class ( WORD | )]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFS7000(config-radsrv)#
```

19.1.17 show

RADIUS Configuration Commands

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Usage Guidelines

To view the show command parameters of RADIUS, refer to radius on page 2-62.

Example

```
RFS7000(config-radsrv)#show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information

  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands

  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands

  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
```

```
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-radsrv)#show
```

20

Wireless Instance

Use the **(config-wireless)** instance to configure the local RADIUS server parameters associated with the wireless controller.

To navigate to this instance, use the following command in the Global Config mode:

```
RFS7000(config)#wireless
RFS7000(config-wireless)#
```

20.1 Wireless Configuration Commands

Table 20.1 gives a summary of Wireless Configuration commands.

Table 20.1 Wireless Configuration Command Summary

Command	Description	Ref.
aap	Invokes *Adaptive AP* (AAP) related commands.	*page 20-4*
admission-control	Enables admission control across all radios.	*page 20-6*
adopt-unconf-radio	Adopts an unconfigured radio. The default template is used for configuration.	*page 20-7*
adoption-pref-id	Defines a preference identifier for the wireless controller. All radios configured with this identifier are more likely to be adopted by this switch.	*page 20-8*
ap	Defines an AP's name and location.	*page 20-9*
ap-containment	Invokes rogue AP containment commands.	*page 20-11*
ap-detection	Invokes access port detection configuration commands.	*page 20-12*
ap-image	Configures new AP image interface.	*page 20-14*
ap-ip	Modifies access port static IP information.	*page 20-15*
ap-standby-attempts-threshold	Reverts the number of attempts after which the standby switch adopts its default value 11.	*page 20-16*
ap-timeout	Changes access port default inactivity timeout value.	*page 20-17*
auto-select-channels	Specifies a list from which channels can be picked.	*page 20-18*
broadcast-tx-speed	Configures the broadcast and multicast traffic transmission rate.	*page 20-19*

Table 20.1 Wireless Configuration Command Summary

Command	Description	Ref.
client	Configures wireless clients.	*page 20-20*
clrscr	Clears the display screen.	*page 20-31*
cluster-master-support	Modifies cluster master support settings, required for cluster-level functioning.	*page 20-32*
country-code	Configures the country of operation. Regulatory configuration (channels, self healing offset) of all configured radios is reset to default values.	*page 20-33*
debug	Initiates debugging functions.	*page 20-34*
dhcp-one-portal-forward	Forwards broadcast DHCP responses to one portal when the destination mobile-unit is known from the response contient.	*page 20-36*
dhcp-sniff-state	Records mobile unit DHCP state information.	*page 20-37*
dot11k	Invokes dot11k related commands	*page 20-38*
end	Ends the current mode and moves to the EXEC mode.	*page 20-39*
exit	Ends the current mode and moves to the previous mode.	*page 20-40*
fix-broadcast-dhcp-rsp	Converts DHCP server broadcast responses to unicast response.	*page 20-41*
hotspot	Reverts hotspot related configuration.	*page 20-42*
help	Describes the interactive help system.	*page 20-43*
load-balance	Disables user load balance.	*page 20-44*
mac-auth-local	Configures the local MAC authentication list.	*page 20-44*
manual-wlan-mapping	Allows manual mapping/un-mapping of WLANs to configured radios.	*page 20-47*
mobile-unit	Configures mobile unit related parameters.	*page 20-48*
mobility	Configures mobility parameters.	*page 20-49*
multicast-packet-limit	Sets a VLAN multicast packet limit.	*page 20-50*
multicast-throttle-watermarks	Configures watermarks for handling bursts of broadcast/multicast frames.	*page 20-51*
no	Negates a command or set its defaults.	*page 20-55*
nas-id	Resets NAS ID.	*page 20-52*
nas-port-id	Resets NAS PORT ID.	*page 20-53*

Table 20.1 Wireless Configuration Command Summary

Command	Description	Ref.
non-preferred-ap-attempts-threshold	Reverts the number of attempts after which the switch adopts non preferred AP to default.	*page 20-54*
proxy-arp	Responds to ARP requests on behalf of mobile units.	*page 20-56*
qos-mapping	Maps QoS between wired and wireless domains.	*page 20-57*
radio	Invokes radio related commands.	*page 20-58*
rate-limit	Sets default rate limit per user.	*page 20-68*
self-heal	Invokes self healing configuration commands.	*page 20-69*
service	Invokes service commands.	*page 20-71*
smart-rf	Configures Smart-RF management parameters.	*page 20-78*
smart-scan-channels	Reverts smart scan channels to default.	*page 20-81*
sensor	Configures *Wireless Intrusion Protection System* (WIPS) server IP address, used to send default configuration to sensors.	*page 20-70*
show	Shows running system information.	*page 20-79*
test	Tests neighbor report on air.	*page 20-82*
wips	Configures WIPS parameters.	*page 20-83*
wlan	Invokes Wireless LAN related commands.	*page 20-87*
wlan-bw-allocation	Allocates radio bandwidth per WLAN.	*page 20-99*

20.1.1 aap

Wireless Configuration Commands

Use this command to invoke *Adaptive AP* (AAP) related commands.

Syntax

```
aap [aap-version|auto-upgrade|config-apply|fwupdate|include-config]

aap aap-version aap7131 <VERSION>

aap auto-upgrade enable

aap config-apply [def-delay <30-10000>|mesh-delay <3-10000>]

aap fwupdate [<1-1024>|<LIST>|filename <FILE>|ipaddress <A.B.C.D>|
  location <FILE-LOCATION>|mode <KEY>|password <KEY>|
  stagger-count <1-10>|unadopted [<1-1024>|<LIST>]|username <KEY>]

aap include-config [snmp|syslog]
```

Parameters

aap (aap-version)	
aap-version aap7131 <VERSION>	Configures the minimum supported AAP version. • aap7131 – Configures the adaptive AP7131 version. • <VERSION> – Configures the minimum AP version required for adoption. Provide the firmware version string in the X.X.X.X-XXXR format.
aap (auto-upgrade)	
auto-upgrade enable	Enables automatic upgrade of adopted AP on the wireless controller.
aap (config-apply)	

config-apply [def-delay <30-10000>| mesh-delay <3-10000>]	Applies AAP configuration settings.
	• def-delay <30-10000> – Sets the time to delay, in seconds, before applying AAP configuration.
	  • <30-10000> – Specify the def-delay time between 30 - 10000 seconds.
	• mesh-delay <3-10000> – Sets the time to delay, in minutes, before applying AAP configuration to Mesh APs.
	  • <3-10000> – Specify the mesh-delay time between 3 - 10000 minutes.

aap (fwupdate)	
fwupdate	Sets AAP firmware upgrade parameters. **Note** 10 AAPs can be simultaneously upgraded at a time using this feature.
<1-1024>	Specify the adaptive AP index between 1 - 1024. Upgrades the firmware of the AP specified by the <1-1024> parameter.

<LIST>	Upgrades APs based on the MAC address provided. You can provide a single MAC address, or a list of MAC indices (for example 1,2,3), or a range of MAC indices (for example, 1-7). **Note:** Use the `show wireless ap` command to view wireless AP indices.
filename <FILE>	Specifies the image file name used for the upgrade.
ipaddress <A.B.C.D>	Specifies the remote *Secure File Transfer Protocol* (SFTP) server's IP address.
location <FILE-LOCATION>	Specifies the image file location on the SFTP server.
mode <KEY>	Specifies the firmware upgrade mode: SFTP .
password <KEY>	Specifies the SFTP server password.
stagger-count <1-10>	Configures the number of simultaneous upgrades possible between 1 - 10.
unadopted [<1-1024>|<LIST>]	Updates unadopted APs. Use one of the following options to specify the AP to update: • <1-1024> – Specify a single AP index between 1 - 1024. • <LIST> – Specify a single AP MAC address, or a list of AP MAC indices (for example, 1,2,3,4), or a range of AP MAC indices (for example, 1-7). **Note:** Use the `show wireless ap-unadopted` command to view unadopted AP list.
username <KEY>	Specify the username to login to the SFTP server.
aap-version (include-config)	
Include-config [snmp|sysylog]	Moves following configuration details to the adopted APs. • snmp – Moves the wireless controller's *Simple Network Management Protocol* (SNMP) configuration (community strings and trap receivers) settings. • syslog – Moves Syslog configuration (Syslog server IP address, enable/ disable syslog, and logging levels) settings.

Example

```
RFS7000(config-wireless)#aap config-apply def-delay 30
RFS7000(config-wireless)#
RFS7000(config-wireless)#aap include-config snmp
RFS7000(config-wireless)#
RFS7000(config-wireless)#aap fwupdate mode sftp
RFS7000(config-wireless)#
```

20.1.2 admission-control

Wireless Configuration Commands

Use this command to enable admission control across all radios.

Syntax

```
admission-control voice [enable]
```

Parameters

voice [enable]	Enables admission control for voice traffic.

Example

```
RFS7000(config-wireless)#admission-control voice enable
RFS7000(config-wireless)#


RFS7000(config-wireless)#show wireless config

country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
ap-detection            : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp one portal forward : disabled
dhcp fix broadcast-rsp  : disabled
broadcast-tx-speed      : optimize-for-range
wlan bw allocation      : disabled
smart-channels used     :
smart-channels excluded :
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
user load balance mode  : disabled

admission control for voice : enabled
cluster-master-support      : enabled
nas-id                      : ""
 -- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-wireless)#
```

20.1.3 adopt-unconf-radio

Wireless Configuration Commands

Use this command to adopt a radio (even if not yet configured). The default template is used for configuration.

Syntax

```
adopt-unconf-radio [enable]
```

Parameters

enable	Enables the adoption of unconfigured radios.

Example

```
RFS7000(config-wireless)#adopt-unconf-radio enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#show wireless config

country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
ap-detection            : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp one portal forward : disabled
dhcp fix broadcast-rsp  : disabled
broadcast-tx-speed      : optimize-for-range
wlan bw allocation      : disabled
-- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-wireless)#
```

20.1.4 adoption-pref-id

Wireless Configuration Commands

Use this command to configure the preference identifier for this switch. Radios configured with this identifier are likely to be adopted by this switch.

Syntax

```
adoption-pref-id <1-65535>
```

Parameters

<1-65535>	Specify a preference ID between 1 - 65535.

Example

```
RFS7000(config-wireless)#adoption-pref-id 100
RFS7000(config-wireless)#

RFS7000(config-wireless)#show wireless config

country-code            : None
adoption-pref-id        : 100
proxy-arp               : enabled
adopt-unconf-radio      : enabled
ap-detection            : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp one portal forward : disabled
dhcp fix broadcast-rsp  : disabled
broadcast-tx-speed      : optimize-for-range
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

20.1.5 ap

Wireless Configuration Commands

Use this command to define the name and location of access ports.

Syntax

```
ap [<1-1024>|<LIST>|<MAC-ADDRESS>]

ap [<1-1024>|<LIST>|<MAC-ADDRESS>][ABG-scan|aap-admin-passwd|
  aap-mgmt-vlan|aap-native-vlan-id|aap-native-vlan-tag|adoption-policy|
  country-code|lan-acl|location|name|radio-config]
```

Parameters

<1-1024>	Specifies a single AP index. Use `show wireless ap` command to view the AP's index value.
<LIST>	Specifies a list or range of AP indices. Use `show wireless ap` command to view the AP's index value.
<MAC-ADDRESS>	Specifies the AP's MAC address in the AA-BB-CC-D-EE-FF format. Use the `show wireless ap` command to view the AP's index value.

[ABG-scan|
aap-admin-passwd|
aap-mgmt-vlan|
aap-native-vlan-id|
aap-native-vlan-tag|
adoption-policy|
country-code|
lan-acl|
location|
name|
radio-config]
	The following keywords are common to the <1-1024>, <LIST>, and <MAC-ADDRESS> parameters:
	• ABG-scan [enable] – Configures ABG scan mode on the AP.
	  • enables – Enables detector radios to perform ABG scan.
	• aap-admin-passwd <LINE> – Configures the AAP admin password.
	  • <LINE> – Specify the password (should be between 1 - 11 characters in length).
	• aap-mgmt-vlan [lan1] [<1-4094>] – Configures the AAP management VLAN.
	  • lan1 <1-4094> – Configures the AAP management VLAN on the LAN1 interface.
	  • <1-4094> – Configures the management VLAN's index between 1 - 4094.
	• aap-native-vlan-id [lan1] [<1-4094>] – Configures native VLAN ID.
	  • lan1 – Configures the native VLAN's ID on the LAN1 interface.
	  • <1-4094> – Configures the native VLAN's ID between 1 - 4094.
	• aap-native-vlan-tag [<1-2>] [tagged|untagged] – Configures the native VLAN's tag.
	  • <1-2> – Specifies the LAN interface (1: LAN1, 2: LAN2).
	  • tagged – Specifies as tagged.
	  • untagged – Specifies as untagged.
	• adoption-policy [allow|deny] – Specifies the adoption policy.
	  • allow – Allows adoption.
	  • deny – Denies adoption.
	• country-code <WORD> – Configures the country of operation.
	  • <WORD> – Specify the 2 letter ISO-3166 country code
	
	Note: Use the `show wireless country-code-list` command to view a list of supported countries. On setting the country code, regulatory configurations (for example, channels and self-healing offset) of configured radios will be reset.
	
	• lan-acl – Applies an ACL on LAN port for AP.
	• location – Configures the AP's location description.
	• name – Configures the AP's name description.
	• radio-config – Sets radio configuration.

Example

```
RFS7000(config-wireless)#ap 00-15-70-14-FE-C4 location 5th Floor SalesUnit
RFS7000(config-wireless)#
```

20.1.6 ap-containment

Wireless Configuration Commands

Use this command to invoke rogue AP containment commands.

Syntax

```
ap-containment [add|enable|interval]

ap-containment [add <MAC-ADDRESS>|enable|interval <20-5000>]
```

Parameters

add <MAC-ADDRESS>	Adds a rogue BSS MAC to the rogue AP containment list. The maximum entries allowed is 256. • <MAC-ADDRESS> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.
enable	Enables protection against rogue access points.
interval <20-5000>	Specifies the time (in milliseconds) between two rogue AP containment procedures.

Example

```
RFS7000(config-wireless)#ap-containment interval 20
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-containment enable
WARNING: Rogue AP Containment should only be used to contain
rogues adversely impacting the network and its devices.
RFS7000(config-wireless)#
```

20.1.7 ap-detection

Wireless Configuration Commands

Use this command to configure access port detection.

Syntax

```
ap-detection [add|detect-wired-rogue|enable|mu-assisted-scan|timeout]
ap-detection add <1-200> [authorized|ignored] [<MAC-ADDRESS>|any] [<SSID>|any]
ap-detection detected-wired-rogue [enable]
ap-detection enable
ap-detection mu-assisted-scan [enable|refesh <300-86400>]
ap-detection timeout [authorized|ignored|unauthorized] <1-65535>
```

Parameters

ap-detection (add)	
add <1-200>	Adds an entry in the authorized or ignored AP list. • <1-200> – Specifies the index where the entry is added. • authorized – Adds this entry in the authorized list. • ignored – Adds this entry in the ignored list. • <MAC-ADRESS> – Adds a specified AP MAC address. Specify the MAC address in the AA-BB-CC-DD-EE-FF format. • any – Adds any MAC address. The following keywords are common to the <MAC-ADDRESS> and 'any' parameters: • <SSID> – Provide an SSID (a string of up to 32 characters). • any – Configures any SSID.
ap-detection (detect-wired-rogue)	
detect-wired-rogue (enable)	Enables detection of rogue APs on the wired network.
ap-detection (enable)	
enable	Starts detection of rogue APs on the wired network.
ap-detection (mu-assisted-scan)	
mu-assisted-scan [enable|refresh]	Configures mobile unit assisted scanning. • enable – Enables mobile unit assisted scanning. • refresh <30-86400> – The period (in seconds) used by all scan-capable mobile units to scan for neighboring APs. • <30-86400> – Specify a value between 30 - 86400 seconds.

ap-detection (timeout)	
timeout [authorized|ignored| unauthorized]	Sets the interval (in seconds) an access port remains in the list after it is no longer seen. Select one of the following options for timeout implementation: • authorized <1-65535> – Configures the timeout, in seconds, for authorized APs. • unauthorized <1-65535> – Configures the timeout, in seconds, for unauthorized APs. • ignored <1-65535> – Configures the timeout, in seconds, for ignored APs.

Example

```
RFS7000(config-wireless)#ap-detection enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection add 150 authorized any any
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection mu-assisted-scan enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection mu-assisted-scan refresh 520
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection timeout authorized 500
RFS7000(config-wireless)#
```

20.1.8 ap-image

Wireless Configuration Commands

Configures the new AP image file location (file path). This path is used to upload the new AP image.

Syntax

```
ap-image [ap100|ap300-ids-sensor|ap300-wisp|ap300-wispe|ap4131|ap5131|
  ap650-wispe|ap7131|revert-ap4131] <FILE-PATH>
```

Parameters

ap-image	Specifies the interface to upload AP images. The following AP images are supported: • ap100 – AP100 AP image • ap300-ids-sensor – AP300 *Intrusion Detection System* (IDS) sensor firmware AP image. • ap300-wisp – AP300 *Wireless Internet Service Provider* (WISP) AP image. • ap300-wispe – AP300 WISPe AP image. • ap4131 – AP4131 AP image • ap5131 – AP5131 adaptive AP image. • ap650-wispe – AP650 WISPe AP image. • ap7131 – AP7131 adaptive AP image. • revert-ap4131 – Reverts AP4131 AP image
<FILE_PATH>	Specify the path of the new file in the following format: Files: flash:/path/file

Example

```
RFS7000(config-wireless)#ap-image ap5131 flash:/aap_10B.bin
RFS7000(config-wireless)#
```

20.1.9 ap-ip

Wireless Configuration Commands

Use this command to modify the static IP address of access ports.

Syntax

```
ap-ip [<LIST>|default-ap]

ap-ip <LIST> [static-ip|switch-ip]
ap-ip <LIST> static-ip <A.B.C.D/M> <A.B.C.D/M>
ap-ip <LIST> switch-ip [add <IP-ADDRESS>|delete [<1-12>|<A.B.C.D>]|set-default]

ap-ip default-ap switch-ip [add <IP-ADDRESS>|delete [<1-12>|<A.B.C.D>]|
  set-default]
```

Parameters

<LIST> [static-ip| switch-ip]	Specify the AP's index/MAC address to modify its static IP address.
	Note: Use the `show wireless ap` command to view the AP's index or MAC address.
	• static-ip <A.B.C.D/M> <A.B.C.D> – Sets the AP's static IP address, netmask and gateway address.
	  • <A.B.C.D/M> – Specify the static IP address and mask in the A.B.C.D/M format.
	  • <A.B.C.D> – Sets the gateway's IP address.
	• switch-ip – Sets the switch's static IP address.
	  • add <LINE> – Adds static switch IP addresses.
	  • <LINE> – The space separated list of static IP address (for example, 192.1168.10.25 10.10.1.4)
	  • delete [<1-12> |<A.B.C.D>] – Deletes specified static switch IP addresses.
	  • <1-12> – Specify the switch's index.
	  • <A.B.C.D> – Specify the switch's IP address in the A.B.C.D format.
	  • set-default – Sets the default switch's IP address.

default-ap switch-ip	Sets the default static switch IP addresses. • add <LINE> – Adds static switch IP addresses. • delete [<1-12>|<A.B.C.D>] – Deletes static switch IP addresses. • set-default – Sets default switch IP addresses.

Example

```
RFS7000(config-wireless)#ap-ip 1 static-ip 192.168.10.25/24 192.168.10.1
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-ip 1 switch-ip add 192.168.10.25 10.10.1.4
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-ip default-ap switch-ip set-default
```

20.1.10 ap-standby-attempts-threshold

Wireless Configuration Commands

Use this command to revert the number of attempts after which the standby switch adopts its default value 11.

Syntax

```
ap-standby-attempts-threshold <5-200>
```

Parameters

<5-200>	Sets the number attempts between 5 - 200.

Example

```
RFS7000(config-wireless)#ap-standby-attempts-threshold 5
RFS7000(config-wireless)#
```

20.1.11 ap-timeout

Wireless Configuration Commands

Use this command to modify the default inactivity timeout period for access port(s).

Syntax

```
ap-timeout <LIST> <40-180>
```

Parameters

<LIST>	An access-port is identified by a single MAC address or by a list of indices. Use `show wireless ap` to view the AP's adopted by the MU and their IP addresses. **Note** If multiple access-ports are specified, each gets a unique IP address.
<40-180>	Specify the new inactivity timeout period between 40 - 180 seconds.

Example

```
RFS7000(config-wireless)#ap-timeout 1 40
RFS7000(config-wireless)#
```

20.1.12 auto-select-channels

Wireless Configuration Commands

Use this command to specify a list from which channels can be picked.

Syntax

```
auto-select-channel [11a|11bg] [<CHANNEL-LIST>|add <CHANNEL-LIST>|
  remove <CHANNEL-LIST>]
```

Parameters

11a	Specifies channel list for the 11a (5GHz) band.
11bg	Specifies channel list for the 11bg (2.4 GHz) band.
<CHANNEL-LIST>	A comma separated list of channels.
add <CHANNEL-LIST>	Adds one or more channels to the existing channel list. • <CHANNLE-LIST> – List the channels to add (comma separated list of channels).
remove <CHANNEL-LIST>	Removes one or more channels to the existing channel list. • <CHANNLE-LIST> – List the channels to remove (comma separated list of channels).

20.1.13 broadcast-tx-speed

Wireless Configuration Commands

Use this command to configure the rate at which broadcast and multicast traffic is transmitted between the switch and mobile units.

Syntax

```
broadcast-tx-speed [range|throughput]
```

Parameters

range	Uses the lowest basic rate. Provides maximum range (this is the default setting).
throughput	Uses the highest basic rate. Provides maximum throughput.

Example

```
RFS7000(config-wireless)#broadcast-tx-speed range
RFS7000(config-wireless)#

RFS7000(config-wireless)#broadcast-tx-speed throughput
RFS7000(config-wireless)#
```

20.1.14 client

Wireless Configuration Commands

Use this command to configure a wireless client.

This command creates an exclude/include list. You will enter the `config-wireless-client-list` instance, and the prompt changes to `create-wireless-client-list#`

Syntax

```
client [exclude-list|include-list] <LIST-NAME>
```

Parameters

exclude-list	Configures a wireless client exclude list.
include-list	Configures a wireless client include list
<LIST-NAME>	Provide a name for the exclude/include list.

Example

```
RFS7000(config-wireless)#client include-list ClientIncList1
RFS7000(config-wireless-client-list)#

RFS7000(config-wireless-client-list)#?
Exclude List Configuration commands:
  clrscr   Clears the display screen
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  no       Negate a command or set its defaults
  service  Service Commands
  show     Show running system information
  station  MU's mac configuration
  wlan     Wireless LAN related commands

RFS7000(config-wireless-client-list)#
```

Table 20.2 summarizes Wireless Client List configuration commands

Table 20.2 Config wireless client list commands summary

clrscr	Clears the display screen.
end	Ends the current mode and moves to the EXEC mode.
exit	Ends the current mode and moves to the previous mode.
help	Describes the interactive help system.
no	Negates or reverts wireless client list commands.
service	Invokes service commands to troubleshoot or debug.
show	Displays current system information.
station	Adds MUs to the exclude/include wireless client list.
wlan	Associates a WLAN with an exclude/include wireless client list.

20.1.14.1 clrscr

Config wireless client list commands summary

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-wireless)#clrscr
RFS7000(config-wireless)#
```

20.1.14.2 end

Config wireless client list commands summary

Use this command to end and exit the `config-wireless-client-list` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-wireless-client-list)#end
RFS7000#
```

20.1.14.3 exit

Config wireless client list commands summary

Use this command to exit the `config-wireless-client-list` mode and move to the previous mode (CONFIG-WIRELESS). The prompt changes to `RFS7000(config-wireless)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-wireless-client-list)#exit
RFS7000(config-wireless)#
```

20.1.14.4 help

Config wireless client list commands summary

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-wireless-client-list)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-wireless-client-list)#
```

20.1.14.5 no

Config wireless client list commands summary

Use this command to negate or revert wireless client list commands.

Syntax

```
no [station|wlan]
```

Parameters

no station	Removes MU's MAC configuration.
no WLAN	Negates WLAN related command.

20.1.14.6 service

Config wireless client list commands summary

Use this command to invoke service commands to troubleshoot or debug `config-wireless-client-list` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show [cli]	Shows the CLI tree of current mode.

Example

```
RFS7000(config-wireless-client-list)#service show cli
Exclude List Configuration mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
        +-WORD [show ip access-group role ( WORD | )]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
```

20.1.14.7 show

Config wireless client list commands summary

Use this command to view current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFS7000(config-wireless-client-list)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-wireless-client-list)#
```

20.1.14.8 station

Config wireless client list commands summary

Use this command to add MUs to the exclude/include wireless client list.

Syntax

```
station <HOST-NAME> [<MAC>|<MAC/MASK>]
```

Parameters

<HOST-NAME>	Defines a name for this host station entry in the exclude/include list. The name should be between 1 -21 characters in length.
<MAC>	Sets the host station's MAC address. Provide the MAC address in one of the following formats: • AA;BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF
<MAC/MASK>	Sets the host station's MAC and mask. Provide the MAC address and mask in one of the following formats: • AA;BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF

Example

```
RFSwitch(config-wireless-client-list)#station ClientIncludeList1 AA:BB:CC:DD:EE:FF
RFSwitch(config-wireless-client-list)#
```

20.1.14.9 wlan

Config wireless client list commands summary

Use this command to associate a WLAN with this exclude/include wireless client list.

Syntax

```
wlan [<1-256>|<WLAN-LIST>]
```

Parameters

<1-256>	Provide a single WLAN's index between 1 - 256.
<WLAN-LIST>	Provide a list of WLAN indices (for example, 1,3,7) or a range of WLAN indices (for example, 3- 7).

Example

```
RFS7000(config-wireless-client-list)#wlan 1
RFS7000(config-wireless-client-list)#
```

20.1.15 clrscr

Wireless Configuration Commands

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-wireless)#clrscr
RFS7000(config-wireless)#
```

20.1.16 cluster-master-support

Wireless Configuration Commands

Use this command to modify cluster master support settings, required for cluster-level functioning.

Syntax

```
cluster-master-support [enable]
```

Parameters

enable	Enables cluster master support, a partial set of configuration will be synchronized with master

Usage Guidelines

Use the `no cluster-master-support enable` command to disable this feature. By default, this feature is disabled.

Example

```
RFS7000(config-wireless)#cluster-master-support enable
RFS7000(config-wireless)#
```

20.1.17 country-code

Wireless Configuration Commands

Use this command to configure the country of operation. This command erases the radio's existing configuration.

Syntax

```
country-code <COUNTRY-CODE>
```

Parameters

<COUNTRY-CODE>	Configures the two letter ISO-3166 country code.

Usage Guidelines

Use the `show wireless country-code-list` command to view the list of supported countries.

Example

```
RFS7000(config)#country-code us
WARNING: Select only the country in which you are using the device.
Any other selection may make the operation of this device illegal.
RFS7000(config)#

RFS7000(config-wireless)#show wireless config

country-code            : us
adoption-pref-id        : 100
proxy-arp               : enabled
adopt-unconf-radio      : enabled
ap-detection            : enabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp one portal forward : disabled
dhcp fix broadcast-rsp  : disabled
broadcast-tx-speed      : optimize-for-range
wlan bw allocation      : disabled
smart-channels used     : 1,6,11,36,40,44,48,149,153,157,161,165
smart-channels excluded : 2,3,4,5,7,8,9,10
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
user load balance mode  : disabled

admission control for voice : enabled
cluster-master-support      : enabled
nas-id                      : ""
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
```

20.1.18 debug

Wireless Configuration Commands

Use this command to initiate cellcontroller debugging functions.

Syntax

```
debug cc [access-port|all|alt|ap-containment|ap-detect|capwap|cluster|
  config|dot11|eap|ids|13-mob|loc-ap|loc-mu|media|mobile-unit|
  radio|radius|self-heal|smart|snmp|system|wips|wisp|wlan] {debug|err|info|warn}
```

Parameters

cc	Displays cellcontroller debugging messages.
access-port	Displays access-port debugging logs
all	Displays all module logs
alt	Displays address lookup logs
ap-containment	Displays rogue AP containment logs
ap-detect	Displays rogue AP detect logs
capwap	Displays *control and provisioning of wireless access points* (capwap) logs
cluster	Displays cluster related logs
config	Displays configuration change logs
dot11	Displays datapath logs
eap	Displays 802.1x/eap logs
ids	Displays intrusion detection logs
13-mob	Displays layer 3 mobility logs
loc-ap	Displays local AP logs
loc-mu	Displays local mobile unit logs
media	Displays encapsulation media logs
mobile-unit	Displays mobile unit logs
radio	Displays radio logs
radius	Displays RADIUS logs
self-heal	Displays self-healing logs
smart	Displays Smart-RF logs
snmp	Displays SNMP logs
system	Displays system call log
wips	Displays *Wireless Intrusion Prevention System* (WIPS) sensor logs
wisp	Displays WISP logs

wlan	Displays WLAN logs
debug	Optional. Displays all messages (default)
err	Optional. Displays error and higher severity messages
info	Optional. Displays information and higher severity messages
warn	Optional. Displays warning and higher severity messages

Example

```
RFS7000(config-wireless)#debug cc wips err

RFS7000(config-wireless)#RFS7000(config-wireless)#debug cc access-port info
RFS7000(config-wireless)#

FS7000(config-wireless)#debug cc wips warn
RFS7000(config-wireless)#
```

20.1.19 dhcp-one-portal-forward

Wireless Configuration Commands

Use this command to forward broadcast DHCP responses to one portal when the destination mobile-unit is known from the response contient.

Syntax

```
dhcp-one-portal [enable]
```

Parameters

enable	Enables forwarding DHCP responses to one portal

Example

```
RFS7000(config-wireless)#dhcp-one-portal-forward enable
RFS7000(config-wireless)#
```

20.1.20 dhcp-sniff-state

Wireless Configuration Commands

Use this command to record mobile unit DHCP state information.

Syntax

```
dhcp-sniff-state [enable]
```

Parameters

enable	Enables the recording of DHCP state information for mobile units

Example

```
RFS7000(config-wireless)#dhcp-sniff-state enable
RFS7000(config-wireless)#
```

20.1.21 dot11k

Wireless Configuration Commands

Use this command to invoke dot11k related commands.

Syntax

```
dot11k send-beacon-req [<1-8192>|<LIST>|mu <MAC-ADDRESS>]
  {measurement-duration <100-1000>}
```

Parameters

send-beacon-req	Triggers the sending of beacon requests.
<1-8192>	Specifies a single mobile unit index between 1 - 8192.
<LIST>	Specifies a list of mobile unit indices (for example, 1,2,3) or a range of mobile unit indices (for example, 1-7)
mu <MAC-ADDRESS>	Specifies mobile unit's MAC address in the AA-BB-CC-DD-EE-FF format.
measurement-duration <100-10000>	Optional. Specifies measurement duration in TUs. • <100-100000> – Specify the measurement duration between 100 - 100000.

Example

```
RFS7000(config-wireless)#dot11k send-beacon-req mu 11-22-33-44-55-66 measurement
-duration 100
% Error: MU is not present
RFS7000(config-wireless)#
```

20.1.22 end

Wireless Configuration Commands

Use this command to end and exit the `config-wireless` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-wireless)#end
RFS7000#
```

20.1.23 exit

Wireless Configuration Commands

Use this command to exit the `config-wireless` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-wireless)#exit
RFS7000(config)#
```

20.1.24 fix-broadcast-dhcp-rsp

Wireless Configuration Commands

Use this command to convert broadcast DHCP server responses to be unicast.

Syntax

```
fix-broadcast-dhcp-rsp [enable]
```

Parameters

enable	Enables support for converting broadcast DHCP server responses to unicast

Example

```
RFS7000(config-wireless)#fix-broadcast-dhcp-rsp enable
RFS7000(config-wireless)#
```

20.1.25 hotspot

Wireless Configuration Commands

Use this command to revert hotspot related configuration. This command adds on or overwrites WLAN hotspot configuration.

Syntax

```
hotspot query <1-10> <WORD> [mu-ip|ssid|switch-ip|switch-name|user-string <WORD>]
```

Parameters

query	Configures query string to be appended to the redirection login URL.
<1-10>	Sets the query index.
<WORD >	Sets the query's field name (for example, userip in ?userip=192.168.0.100).
mu-ip	Sets the mobile unit's IP address.
ssid	Specifies the WLAN's SSID.
switch-ip	Sets the switch's router IP address for external hotspot server.
switch-name	Sets the switch's name.
user-string <WORD>	Sets the query value as user-string. • <WORD> – Specify the user string used as the query value.

```
Example
  RFS7000(config-wireless)#hotspot query 1 192.168.0.100 ssid
  RFS7000(config-wireless)#
```

20.1.26 help

Wireless Configuration Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-wireless)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-wireless)#
```

20.1.27 load-balance

Wireless Configuration Commands

Use this command to set the user load balance mode.

Syntax

```
load-balance [by-count|by-throughput]
```

Parameters

by-count	Sets load balance by user account.
by-throughput	Sets load balance by radio throughput (threshold 1Mbps)

Example

```
RFS7000(config-wireless)#load-balance by-throughput
RFS7000(config-wireless)#
```

20.1.28 mac-auth-local

Wireless Configuration Commands

Use this command to configure the local MAC authentication list.

Syntax

```
mac-auth-local <1-1000> [allow|deny|rate-limit]

mac-auth-local <1-1000> allow <STARTING-MAC-ADDRESS> <ENDING-MAC-ADDRESS>
  [<WLAN-LIST>|not-mapped] {<WORD>|zone [<1-48>|default|unknown]}

mac-auth-local <1-1000> deny <STARTING-MAC-ADDRESS> <ENDING-MAC-ADDRESS>
  [<WLAN-LIST>|not-mapped] {<WORD>|zone [<1-48>|default|unknown]}

mac-auth-local <1-1000> rate-limit [wired-to-wireless|wireless-to-wired]
  <100-1000000>
```

Parameters

<1-1000>	Sets the entry index between 1 - 1000.
mac-auth-local <1-1000> (allow)	
allow	Allows mobile units that match this rule to associate. • <STARTING-MAC-ADDRESS> – The starting MAC address in the AA-BB-CC-DD-EE-FF format. • <ENDING-MAC-ADDRESS> – The ending MAC address in the AA-BB-CC-DD-EE-FF format. • <WLAN-LIST> – Specifies a list (for example, 1,3,7) or range (fore example, 3-7) of WLAN indices. • not-mapped – Specifies an unmapped row. • <WORD> – Optional. radio description substring. • zone [<1-48>|default|unknown] – Optional. The GeoFencing location zone for devices matching this ACL rule. •<1-48> – The administrator defined zone ID. •default – Specifies the user is located within the site in the default zone. •unknown – Specifies the users location is currently unknown or out of bounds of the site.

mac-auth-local <1-1000> (deny)	
deny	Denies association to mobile units that match this rule. • <STARTING-MAC-ADDRESS> – The starting MAC address in AA-BB-CC-DD-EE-FF format. • <ENDING-MAC-ADDRESS> – The ending MAC address in AA-BB-CC-DD-EE-FF format. • <WLAN-LIST> – Specifies a list (for example, 1,3,7) or range (for example, 3-7) of WLAN indices. • not-mapped – Specifies an unmapped row. • <WORD> – Optional. The radio description substring. • zone [<1-48>|default|unknown]– Optional. The GeoFencing location zone for devices matching this ACL rule. •<1-48> – The administrator defined zone ID. •default – Specifies the user is located within the site in the default zone. •unknown – Specifies the users location is currently unknown or out of bounds of the site.
rate-limit	Sets the rate limit for this ACL entry. • wired-to-wireless <100-1000000> – Sets the rate limit for the down link direction - from network to wireless client. • wireless-to-wired <100-1000000> – Sets the rate limit for the up link direction - from wireless client to network. • <100-1000000> – Specify the rate between 100 - 1000000 Kbps.

Example

```
RFS7000(config-wireless)#mac-auth-local 452 allow 12.11.11.120 12.11.11.150 3-7
TestString zone 1
RFS7000(config-wireless)#
RFS7000(config-wireless)#mac-auth-local 1 rate-limit wired-to-wireless 100
RFS7000(config-wireless)#
```

20.1.29 manual-wlan-mapping

Wireless Configuration Commands

Use this command to manually map/un-map WLANs configured on a radio.

Syntax

```
manual-wlan-mapping [enable]
```

Parameters

enable	Enables support for manual WLAN mapping

Example

```
RFS7000(config-wireless)#manual-wlan-mapping enable
RFS7000(config-wireless)#
```

20.1.30 mobile-unit

Wireless Configuration Commands

Use this command to configure mobile unit related parameters.

Syntax

```
mobile-unit [association-history|probe-history]

mobile-unit association-history [clear|enable]
mobile-unit probe-history [add <1-200> <MAC-ADDRESS>|enable]
```

Parameters

association-history [clear|enables]	Configures a mobile unit's association history logging parameters. • clear – Clears the association history for all mobile-units. • enable – Enables the mobile unit's association history logging.

probe-history [add|enable]	Configures a mobile unit's probe history logging parameters.
	• add <1-200> – Adds a mobile unit for probe history logging.
	  • <1-200> – Specify the mobile unit's index between 1 - 200 to add probe logging MAC.
	  • <MAC-ADDRESS> – The MAC address of the mobile.
	• enable – Enables mobile unit probe logging.

Example

```
RFS7000(config-wireless)#mobile-unit probe-history enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobile-unit association-history enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobile-unit probe-history add 20 AA-BB-CC-DD-EE-FF
RFS7000(config-wireless)#
```

20.1.31 mobility

Wireless Configuration Commands

Use this command to configure mobility parameters.

Syntax

```
mobility [enable|local-address|max-roam-period|peer]

mobility local-address <A.B.C.D>

mobility max-roam-period <1-300>

mobililty peer <A.B.C.D>
```

Parameters

enable	Enables mobility globally.
local-address <A.B.C.D>	Sets the local address for mobility. • <A.B.C.D> – Specify the IP address in the A.B.C.D format.
max-roam-period <1-300>	Sets the maximum roam period for a mobile unit between 1 - 300 seconds.
peer <A.B.C.D>	Adds a peer to this mobility region. • A.B.C.D – Specify the peer's IP address.

Example

```
RFS7000(config-wireless)#mobility enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobility local-address 12.12.12.1
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobility max-roam-period 10
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobility peer 157.208.235.108
RFS7000(config-wireless)#
```

20.1.32 multicast-packet-limit

Wireless Configuration Commands

Use this command to a configure multicast packet limit per second for a VLAN.

Syntax

```
multicast-packet-limit <0-128> [<1-4094>|<VLAN-RANGE>]
```

Parameters

<0-128> [<1-4094> | <vlan range>]	Sets the multicast packet limit per second between 0 - 128. After specifying the rate limit specify the VLAN using one of the following options: • <1-4094> – Single VLAN ID (1-4094) that the new limit applies to • <VLAN-RANGE> – A list (1,3,7) or range (3-7) of VLAN IDs

Example

```
RFS7000(config-wireless)#multicast-packet-limit 120 50
RFS7000(config-wireless)#multicast-packet-limit

RFS7000(config-wireless)#multicast-packet-limit 120 1,10,25 RFS7000(config-
wireless)#multicast-packet-limit
```

20.1.33 multicast-throttle-watermarks

Wireless Configuration Commands

Use this command to configure watermarks for handling bursts of broadcast/multicast frames.

Syntax

Parameters`multicast-throttle-watermarks [low <0-100>] [high <0-100>]`

low <0-100>	Configures the low water-mark. If the percentage of free packets in the system is lower than this threshold, the incoming frame will be dropped.
high <0-100>	Configure the high water-mark. If the percentage of free packets in the system is between the low water-mark and this value, the packet is subjected to a random-early-drop. If free packets are greater than this value, the packet is processed.

Example

```
RFS7000(config-wireless)#multicast-throttle-watermarks low 10 high 20
RFS7000(config-wireless)#
```

20.1.34 nas-id

Wireless Configuration Commands

Use this command to reset *Network Access Server* (NAS) ID.

Syntax

```
nas-id <WORD>
```

Parameters

<WORD>	Specify the NAS ID (a string up to 256 characters in length).

Example

```
RFS7000(config-wireless)#nas-id 12
RFS7000(config-wireless)#
```

20.1.35 nas-port-id

Wireless Configuration Commands

Use this command to reset NAS port ID.

Syntax

```
nas-port-id <WORD>
```

Parameters

<WORD>	Specify the NAS port ID (a string up to 256 characters).

Example

```
RFS7000(config-wireless)#nas-port-id 23
RFS7000(config-wireless)#
```

20.1.36 non-preferred-ap-attempts-threshold

Wireless Configuration Commands

Use this command to revert the number of attempts after which the switch adopts non preferred AP to its default value 0.

Syntax

```
non-preferred-ap-attempts-threshold <0-20>
```

Parameters

<0-20>	Specify the number of attempts between 0 - 20.

Example

```
RFS7000(config-wireless)#non-preferred-ap-attempts-threshold 1
RFS7000(config-wireless)#
```

20.1.37 no

Wireless Configuration Commands

Use this command to negate a command or set its defaults.

Syntax

```
no [aap|admission-control|adopt-unconf-radio|adoption-pref-id|ap|ap-containment|
  ap-detection|ap-image|ap-ip|ap-standby-attempts-threshold|ap-timeout|
  auto-select-channels|broadcast-tx-speed|client|cluster-master-support|country-code|
  debug|dhcp-one-portal-forward|dhcp-sniff-state|fix-broadcast-dhcp-rsp|
  hotspot|load-balance|mac-auth-local|manual-wlan-mapping|mobile-unit|
  mobility|multicast-packet-limit|multicast-throttle-watermarks|nas-id|nas-port-id|
  non-preferred-ap-attempts-threshold|proxy-arp|qos-mapping|radio|rate-limit|
  self-heal|sensor|service|smart-scan-channels|wips|wlan|wlan-bw-allocation]
```

Parameters

Refer to *Table 20.1 on page 20-1* for the parameters negated using the **no** command.

Example

```
RFS7000(config-wireless)#no mobility enable
RFS7000(config-wireless)#
```

20.1.38 proxy-arp

Wireless Configuration Commands

Use this command to respond to ARP requests on behalf of mobile units.

Syntax

```
proxy-arp [enable]
```

Parameters

enable	Enables support for proxy ARP.

Example

```
RFS7000(config-wireless)#proxy-arp enable
RFS7000(config-wireless)#
```

20.1.39 qos-mapping

Wireless Configuration Commands

Use this command to configure *Quality of Service* (QoS) mappings between wired and wireless domains.

Syntax

```
qos-mapping [wired-to-wireless|wireless-to-wired]

qos-mapping wired-to-wireless [dot1p <0-7>|dscp <0-63>]
   [<0-7>/<0-63>|tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7]

qos-mapping wireless-to-wired [tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7] [dot1p <0-7>]
```

Parameters

wired-to-wireless	Mappings used while switching wired traffic over the air. • dot1p <0-7> – Configures the mapping of 802.1p tags to access categories. Specify more than one 802.1p tag (0-7) if needed. • dscp <0-63> – Configures the mapping of DSCP values to access categories. Specify more than one DSCP value (0-63) if needed. The following keywords are common to the dot1p and DSCP parameters: • tid0 – best effort category traffic • tid1 – background category traffictid2 background category traffic • tid3 – best effort category traffic • tid4 – video traffic category traffic • tid5 – video traffic category traffic • tid6 – voice traffic category traffic • tid7 – voice traffic category traffic
wireless-to-wired	Mappings used while switching wireless traffic to rest of the network. • tid0 – best effort category traffic • tid1 – background category traffictid2 background category traffic • tid3 – best effort category traffic • tid4 – video traffic category traffic • tid5 – video traffic category traffic • tid6 – voice traffic category traffic • tid7 – voice traffic category traffic • dotp1 <0-7> – Configures the 802.1p tags that corresponds to selected wireless traffic ID.Specify more than one 802.1p tag (0-7) if needed.

Example

```
RFS7000(config-wireless)#qos-mapping wireless-to-wired tid0 dot1p 5
RFS7000(config-wireless)#
```

20.1.40 radio

Wireless Configuration Commands

Use this command to configure radio related settings.

Syntax

```
radio [<1-4096>|<RADIO-INDEX-LIST>|add|all-11a|all-11an|all-11b|all-11bg|all-11bgn|
  configure-8021X|default-11a|default-11an|default-11b|default-11bg|
  default-11bgn|dns-name]

radio [<1-4096>|<RADIO-INDEX-LIST>|all-11a|all-11an|all-11b|all-11bg|all-11bgn]
  [admission-control|adoption-policy|adoption-pref-id <0-65535>|ampdu|antenna-mode|
  base-bridge|beacon-interval <50-200>|bridge-fwd-delay <4-30>|bridge-hello <1-10>|
  bridge-max-ageout <4-3600>|bridge-msg-age <6-40>|bridge-priority <0-65535>|
  bss|channel-power|client-bridge|copy-config-from|description <LINE>|detector|
  dot11k [enable|quiet-element]|dtim-period|enforce-spec-mgmt [enable]|
  enhanced-beacon-table|enhanced-probe-table|group-id <1-256>|location-message <LINE>|
  mac <MAC-ADDRESS>|max-mobile-units <1-256>|mesh-associations <1-3>|
  moto-simple-voice [enable]|mu-power <0-20>|nas-id <WORD>|nas-port-id <WORD>|
  on-channel-scan|radio-number <0-3>|reset|reset-ap|rf-mode|rss [enable]|
  rts-threshold <0-2346>|run-acs|self-heal-offset <0-30>|
  short-gi [enable]|short-preamble|speed|timeout <40-180>|
  tunnel [tx-rate-class <1-4>]|wmm]

radio <1-4096> admission-control voice [max-mus <0-256>|max-perc <0-100>|
  max-roamed-mus <0-256>|res-roam-perc <0-100>]

radio <1-4096> adoption-policy [allow|deny]

radio <1-4096> ampdu [min-spacing|rx-limit|tx-enable|tx-limit]
configure-8021
radio <1-4096> antenna-mode [diversity|mimo|primary|secondary]

radio <1-4096> bss [<1-4>|add-wlans|auto] <WLAN-LIST>

radio <1-4096> channel-power [indoor|outdoor] [<1-200>|acs|random] <4-20>

radio <1-4096> client-bridge [bb-radio <1-16>|bridge-select-mode [auto|manual]|
  enable|mesh-timeout [0|1|<2-200>]|ssid <SSID>]

radio <1-4096> copy-config-from [<1-1000>|default-11a|default-11b|default-11bg]

radio <1-4096> dtim-period <1-50> {bss <1-4>}

radio <1-4096> wmm [background|best-effort|video|voice]
  [aifsn <1-15>|burst <0-65535>|cw <0-15>]

radio add <1-4096> <MAC-ADDRESS> [11a {ap300}|11an {aap7131}|
  11bg {ap300}|11bgn {aap-7131}]

radio configure-8021x <USER-NAME> <PASSWD> {<AA-BB-CC-DD-EE-FF>}

radio dns-name <DNS-NAME> {<AA-BB-CC-DD-EE-FF>}
```

Parameters

radio (<1-4096>)	
<1-4096>	Defines a single radio index
admission-control [voice]	Configures the following admission control parameters for voice traffic: • max-mus <0-256> – The maximum mobile units to be admitted. Specify a value between 0 -256. • max-perc <0-100> – The maximum percentage of air time allocated to voice traffic. Specify a value between 0 - 100%. • max-roamed-mus <0-256> – The maximum roamed mobile units to be admitted. Specify a value between 0 - 256. • res-roam-perc – The percentage of air time allocated exclusively for roamed mobile-unit.This value <0-100> is calculated relative to the configured max air time percentage allocated for voice traffic.
adoption-policy [allow|deny]	Specifies the adoption policy for this radio. • allow – Allows adoption. • deny – Denies adoption.
adoption-pref-id <0-65535>	Specifies the preference identifier for this radio. The radio is more likely to be adopted by a preferred switch. **Note:** An AP300 has two radio's. Configuring any one radio as a pref-id ensures the other radio is also configured with this pref-id. An AP300 cannot be adopted by two switches simultaneously.

ampdu [min-spacing| rx-limit|tx-enable|tx-limit]	Configures the MAC protocol frames.
	• min-spacing – Specifies the spacing between received MPDUs. The values are as follows:
	  • .25 microsec
	  • .5 microsec
	  • 0 microsec
	  • 1 microsec
	  • 2 microsec
	  • 4 microsec
	  • 8 microsec
	• rx-limit –Specifies the receive buffer limit. The values are as follows:
	  • 16382 bytes
	  • 32767 bytes
	  • 65535 bytes
	  • 8191 bytes
	• tx-enable [min-spacing|rx-limit|tx-limit] – Enables transmit A-MPDU
	• tx-limit <0-65535> – Sets the transmit buffer limit between 0 - 65535.

antenna-mode [diversity|mimo|primary| secondary]	Defines the antenna diversity mode. Select from the following options: • diversity– Full diversity (both antennas) • mimo – MIMO • primary– Primary antenna only • secondary– Secondary antenna only **Note:** Before executing this command, ensure the radio is present and is an AP300.
base-bridge [enable|max-clients]	Configures the base bridge settings. • enable – Enables this radio to act as the base bridge and accept connections from client bridges. • max-clients <0-12> – Configures the maximum number of client bridges allowed.
beacon-interval <50-200>	Sets the beacon interval in K-uSec.
bridge-fwd-delay <4-30>	Sets the STP bridge forward delay time in seconds.
bridge-hello <1-10>	Sets the STP bridge hello time in seconds.
bridge-max-ageout <4-3600>	Sets the STP bridge maximum ageout time in seconds.
bridge-msg-age <6-40>	Sets the STP bridge message age in seconds.

bridge-priority <0-65535>	Sets the STP bridge priority value
bss [<1-4>|add-wlans|auto] <WLAN-LIST>	Maps wireless LANs to radio BSSID's • <1-4> – Sets the BSS ID where a wireless LAN is mapped. • add-wlans – Adds new WLANs to existing radios (this is a partial change and other WLANs on the radio are left as is) • auto – Configures automatic assignment of BSS. If the user selects WLANs the system automatically assigns them to a BSS. The following keyword is common to all of the above parameters: • <WLAN-LIST> – A list (1,3,7) or range (3-7) of WLAN indices. When a BSS is specified, the first WLAN is used as the primary WLAN. When the auto option is used, the system automatically assigns the first four WLANs as primaries on their respective BSS's.
channel-power [indoor|outdoor] [<1-200>|acs|random] <4-20>	Sets the location, channel, and transmit power level for this radio. • indoor – Defines location as indoor. • outdoor – Defines location as outdoor. The following keywords are common to the indoor and outdoor parameters: • <1-200> – Sets the channel number • acs – Configures *auto channel selection* (acs). The radio scans for the least congested channel at startup or at reconfiguration. • random – Configures random channel selection • <4-20> – Sets the radio power in dBm The following keywords are applicable to the <1-200>, acs, and random parameters: • lower – Optional. Configures lower channel width mode. • higher – Optional. Configures higher channel width mode. • 20MHz – Optional. Configures the 20Mhz width mode. • 40MHz – Optional. Configures the 40 Mhz width mode.

client-bridge [bb-radio| bridge-select-mode| enable|mesh-timeout|ssid]	Configures client bridge capability.
	• bb-radio <1-16> <MAC-ADDRESS> – Adds the preferred *base bridge* (bb) details.
	  • <1-16> – The priority value of the connection.
	  • <MAC-ADDRESS> – Specify the MAC address.
	• bridge-select-mode [auto|manual] – Configures the base bridge selection mode.
	  • auto – Automatically selects base bridge.
	  • manual – Manually selects the base bridge.
	• Enable – Enables client bridge capability.
	• mesh-timeout [0|1 <2-200>] – Configures the client bridge link timeout value.
	  • 0 – Disables uplink detection.
	  • 1 – Uplink detect – shutdowns when all mesh-backhaul links are down.
	  • <2-200> – Sets the timeout period between 2 - 200 seconds.
	• ssid <SSID> – Sets the WLAN's ESSID to use.
	  • <SSID> – SSID for mesh (a string up to 32 characters in length)

copy-config-from [<1- 4096>|default-11a| default-11b|default-11bg]	Copies the configuration from a previously configured radio. • <1- 4096> – Specify the radio index to copy configuration from. • default-11a – Uses the default 11a configuration template. • default-11b – Uses the default 11b configuration template. • default-11bg – Uses the default 11bg configuration template.
description <LINE>	Configures the radio's description (should not exceed 20 characters in length).
detector	Dedicates this radio as a detector. No mobile units can associate to a detector.

dot11k [enable|quiet-element]	DOT11k related commands.
	• enable – Enables 802.11k for the radio (only for AP300)
	• quiet-element [defaults|duration|enable] – Configures quiet element parameters
	  • defaults – Sets to default.
	  • duration <20-150> [interval <200-255>] – Sets the time to remain quiet in TUs.
	  • <20-150> – Specify the quiet time in K-u seconds.
	  • interval <200-255> – Configures the number of beacons after which the quiet element is sent.
	  • enable – Enables the quiet element.

dtim-period <1-50> {bss <1-4>}	Sets the *Delivery Traffic Indication Message* (DTIM) period (number of beacons between successive DTIMs) • <1-50> – Specify the DTIM period between 1 - 150. • bss <1-4> – Optional. Configures the BSS index between 1 - 4.
enforce-spec-mgmt (enable)	Enforces spectrum management checks on this radio. Only mobile units that advertise spectrum management are allowed to associate to this radio.
enhanced-beacon-table	Enables enhanced beacon table for AP locationing
enhanced-probe-table	Enables enhanced probe table for MU locationing
group-id <1-256>	Specifies the radio groups to balance user load • <1-256> – The radio group identifier for this access-port
location-message <LINE>	Specifies a message sent to mobile units associated with the radio. This message must not exceed 80 characters in length.
mac <AA-BB-CC-DD-EE-FF>	Changes the parent (access port) MAC address of the radio. • <AA-BB-CC-DD-EE-FF> – The MAC address in AA-BB-CC-DD-EE-FF format.
max-mobile-units <1-256>	Sets the maximum number of mobile units allowed to associate with this radio.
mesh-associations <1-3>	Specifies the number of client bridge mesh associations between 1 - 3.
moto-simple-voice (enable)	Enables Motorola Simple Voice - use the WMM voice queue as a strict priority voice queue.
mu-power <0-20>	Configures the power adjustment level for mobile units associated with this access port. Mobile units that support this element must reduce their transmit power by the specified value. • <0-20> – Specify the power in dBm.
nas-id <WORD>	Configures a NAS-ID for this radio
nas-port-id <WORD>	Configures a NAS-PORT-ID for this radio
on-channel-scan	Enables rogue scanning on this radio
radio-number <0-3>	Specifies the radio number inside AP. Enter 0 or omit when there is no ambiguity. The AP uses this value to differentiate between like radios.
reset	Resets a radio (resets the specified radio and not the complete access port)
reset-ap	Resets the parent access port (this resets all radios on that access port)

rf-mode	Configures radio speed based on 802.11 mode selected • a – a only mode • an – a and n modes • b – b only mode • bg – b and g modes • bgn – b, g and n modes • custom – custom • g – g only mode • n – n only mode
rts-threshold <0-2346>	Sets the *Request to Send* (RTS) threshold between0 - 2346 bytes.
run-acs	Runs *auto channel selection* (ACS) on this radio. The radio must already have been configured for ACS
self-heal-offset <0-30>	Configures the self healing offset, measured in dBm, for regulatory compliance **Note:** This offset is based off the regulatory maximum power for the specified channel (the command "`show wireless regulatory`" shows the max power allowed)
short-gi [enable]	Enables *Short Guard Interval* (Short GI) capability for both the 20 MHz and the 40 MHz channels for the 11n radio.
short-preamble	Enables short preamble support **Note:** This command disables support for long preamble. Mobile Units that only support long preamble will not be able to associate.

speed	Configures the basic and supported data rates • 1 1-Mbps. • 11 11-Mbps • 12 12-Mbps • 18 18-Mbps • 2 2-Mbps • 24 24-Mbps • 36 36-Mbps • 48 48-Mbps • 54 54-Mbps • 5.5 5.5-Mbps • 6 6-Mbps • 9 9-Mbps • basic1 basic 1-Mbps • basic11 basic 11-Mbps • basic11a rate set (6,12,24 Mbps) • basic11an rate set (6,12,24, MCS 0-7) • basic11b1 rate set (1 and 2 Mbps) • basic11b2 rate set (1,2,5.5,11 Mbps) • basic11bg rate set (1,2,5.5,11,6,12,24 Mbps) • basic11bgn rate set (1,2,5.5,11,6,12,24, MCS 0-7) • basic11g rate set (6,12,24 Mbps) • basic11gn rate set (6,12,24, MCS 0-7) • basic11n rate set (MCS 0-7) • basic12 basic 12-Mbps • basic18 basic 18-Mbps • basic2 basic 2-Mbps • basic24 basic 24-Mbps • basic36 basic 36-Mbps • basic48 basic 48-Mbps • basic54 basic 54-Mbps • basic5p5 basic 5.5-Mbps • basic6 basic 6-Mbps • basic9 basic 9-Mbps • default Factory default rates based on radio type • range All rates enabled, the lowest one set to basic • throughput All rates basic (note: only g clients allowed on 11bg radios)
timeout <40-180>	Specifies timeout value in seconds.
tunnel [tx-rate-class <1-4>]	Configures the tunnel transmit rate class for this radio. • tx-rate-class <1-4> – Specify the transmit rate class number.

wmm [background| best-effort|video|voice] (aifsn <1-15>| burst <0-65535>| cw <0-15>)	Sets 802.11e / *Wireless MultiMedia* (WMM) parameters (supported only on AP300) • background – Prioritizes background category traffic • best-effort– Prioritizes best effort category traffic • video – Prioritizes video traffic category traffic • voice – Prioritizes voice traffic category traffic The following keywords are common to all traffic types: • aifsn <1-15> – Sets the *Arbitration Inter Frame Spacing Number* (AIFSN), which is the wait time in milliSeconds between data frames derived using AIFSN and the slot-time. • burst <0-65535> – Sets the transmit-opportunity value. An interval when a particular WMM mobile unit has the right to initiate transmissions on the wireless medium. • cw <0-15> – Sets *Contention Window* (cw) parameters. Select a number between 0 and the minimum contention window to wait before re-attempting a transmission. MUs then double their wait time on a collision, until it reaches the maximum contention window.
radio <RADIO-INDEX-LIST>	
<RADIO-INDEX-LIST>	A list (3,7) or range (3-7) of radio indices.
radio (add)	

add <1-4096> <MAC-ADDRESS> [11a{ap300}| 11an {aap7131} 11bg {ap300}| 11bgn {aap7131}]	Adds a new radio
	• <1-4096> <MAC-ADDRESS> – The radio's index.
	  • <MAC-ADDRESS> – The radio's MAC address in AA-BB-CC-DD-EE-FF format.
	Select the radio type from the following:
	• 11a – 802.11a type radio
	• 11an – 802.11an type radio
	• 11bg – 802.11bg type radio.11bgn – 802.11bgn type radio
	  • ap300 – Optional. Access port type AP300 (default for 11a and 11bg)
	  • aap7131 – Optional. Access-port type Adaptive AP7131

all-11a	All 11a radios currently in configuration
all-11an	All 11an radios currently in configuration
all-11b	All 11b radios currently in configuration
all-11bg	All 11bg radios currently in configuration
all-11bgn	All 11bgn radios currently in configuration

configure-8021X <USER-NAME>	Configures the 802.1X username and password on adopted access port. • <USER-NAME> – Specify the user name. • <PASSWD> – Specify the 802.1x password the access ports must use. • <MAC-ADDRESS> – Optional. Specify the access port MAC address. The system changes the username and password only on the access port with the specified MAC address. If not specified, the user name and password are sent to all currently adopted access ports.
default-11a	Uses the default 11a configuration template
default-11an	Uses the default 11an configuration template
default-11b	Uses the default 11b configuration template
default-11bg	Uses the default 11bg configuration template
default-11bgn	Uses the default 11bgn configuration template
dns-name <DNS-NAME> {<MAC-ADDRESS>|	Configures the DNS name used in the L3 Discovery of adopted access ports • <AA-BB-CC-DD-EE-FF> – Optional. Changes the DNS name on only the access port with the specified MAC address. If not specified, the DNS name update is sent to all adopted access ports.

Example

```
RFS7000(config-wireless)#radio 250 bss auto 3-5
RFS7000(config-wireless)#

RFS7000(config-wireless)#radio 1 channel-power indoor 1 16
Regulatory parameter values depend on country of operation and radio type.
 Refer to documentation for more regulatory information
RFS7000(config-wireless)#

RFS7000(config-wireless)#radio 1 antenna-mode diversity
RFS7000(config-wireless)#
```

20.1.41 rate-limit

Wireless Configuration Commands

Use this command to set default rate limit per user.

Syntax

```
rate-limit [wired-to-wireless|wireless-to-wired]
```

Parameters

wired-to-wireless <100-1000000>	Configures the rate limit in the down link direction - from network to wireless client • <100-1000000> – Rate in the range of <100-1000000> kbps
wireless-to-wired <100-1000000>	Configures the rate limit in the up link direction - from wireless client to network • <100-1000000> – Rate in the range of <100-1000000> kbps

Example

```
RFS7000(config-wireless)#rate-limit wireless-to-wired 100
RFS7000(config-wireless)#
```

20.1.42 self-heal

Wireless Configuration Commands

Use this command to configure self healing parameters.

Syntax

```
self-heal [interference-avoidance|neighbor-recovery]

self-heal interference-avoidance [enable|hold-time <30-65535>|retries <0.0-15.0>]

self-heal neighbor-recovery [action|enable|neighbors|run-neighbor-detect]
self-heal neighbor-recovery action [both|none|open-rates|raise-power]
  radio [<1-4096>|<RADIO-LIST>]
self-heal neighbor-recovery neighbors <1-4096> [<1-4096>|<RADIO-LIST>]
```

Parameters

interference-avoidance [enable| hold-time|retries]	Configures interference avoidance parameters. • enable – Enables/disables interference avoidance. • hold-time <30-65535> – The interval (in seconds) to disable interference avoidance after a detection. This prevents a radio from changing channels continuously. Set the hold-time between 0 - 65535 seconds. • retries <0.0-15.0> –Sets the average number of retries to force a radio to re-run auto channel selection. Set a value between 0 - 15.

neighbor-recovery [action|enable|neighbors |run-neighbor-detect]	Configures neighbor recovery parameters.
	• action [both|none|open-rates|raise-power] radio (<1- 4096>|<RADIO-LIST>) – Radio self healing action when neighbors are detected down
	  • both – Raises the power to max and open all rates
	  • none – Does nothing
	  • open-rates – Opens all rates
	  • raise-power – Raises the power to max
	  • radio – Modifies the action for specified radio(s)
	  • <1-4096> – A single radio index
	  • <RADIO-LIST> – A list (1,3,7) or range (3-7) of radio indices
	• enable – Monitors access ports and attempts to increase coverage on failure
	• neighbors <1-1000> (<1- 4096>|<RADIO-LIST>) – Adds radios as neighbors
	• run-neighbor-detect – Disassociates mobile units, clears current neighbors and runs neighbor detection

Example

```
RFS7000(config-wireless)#self-heal interference-avoidance enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#self-heal interference-avoidance hold-time 600
RFS7000(config-wireless)#

RFS7000(config-wireless)#self-heal neighbor-recovery enable
Note: reducing the configured transmit power of radios will ensure
that there is room to increase power when a neighbor fails
RFS7000(config-wireless)#

RFS7000(config-wireless)#self-heal neighbor-recovery neighbors 1 1
RFS7000(config-wireless)#
```

20.1.43 sensor

Wireless Configuration Commands

Use this command to configure WIPS server IP address, used to send default configuration to sensors when they are configured.

Syntax

```
sensor default-config [wips-server-ip [primary <IP-ADDRESS>|secondary <IP-ADDRESS>]]
```

Parameters

default-config	The default configuration sent to sensors when they are configured.
wips-server-ip {primary|secondary}	Specifies the WIPS server's IP address. • primary <A.B.C.D> – Configures the primary WIPS server. • secondary <A.B.C.D> – Configures the secondary WIPS server. • <IP-ADDRESS> – Specify the primary/secondary WIPS server's IP address in A.B.C.D format.

Example

```
FS7000(config-wireless)#sensor default-config wips-server-ip primary 1.0.2.3
RFS7000(config-wireless)#
```

20.1.44 service

Wireless Configuration Commands

Use this command to invoke service commands to troubleshoot or debug the `(config-wireless)` instance configuration.

Syntax

```
service [clear|show|smart-rf|wireless]

service clear wireless mobile-unit association-statistics

service show [cli|radio-neighbor|smart-rf|wireless <OPTIONS>]
service show radio-neighbor [mu <MAC-ADDRESS>]
service show smart-rf [debug-config|sensitivity [mu {<1-8192>|<MAC-ADDRESS>}|
  pattern [pattern-11a|pattern-11b|pattern-bg|pattern-2-mbps]|rates <RATE-FLAGS>]

service show wireless [ap-history {<XX-XX-XX-XX-XX-XX>}|buffer-counters|
  enhanced-beacon-table [config|report]|enhanced-probe-table [config|report]|
  group <1-256>|group-stats|legacy-load-balance|mu-cache-buckets|
  mu-cache-entry {<1-8192>|<MAC-ADDRESS>}|mvlan <1-256>|
  radio{<1-4096>|description|mapping}|radio-cache-entry {<MAC-ADDRESS>}|
  radio-hash-buckets|vlan-cache-buckets|vlan-cache-entry {<1-8192>|<MAC-ADDRESS>}|
  waiting {<0-99>}]

service smart-rf [clear-history|load-from-file|replay|rescue|restore|
  save-to-file|simulate]
service smart-rf [replay [enable]|rescue <MAC-ADDRESS>|restore <MAC-ADDRESS>|
  simulate [coverage-hole <1-4096> <UNIT_RANGE>|interference <MAC-ADDRESS>]

service wireless [ap-history [clear|enable]|clear-ap-log {<1-1024>}|
  custom-cli [sh-wi-mobile-unit|sh-wi-radio]|dot11i [enforce]|
  enhanced-beacon-table|enhanced-probe-table|forward-eap-to-wired|
  free-packet-watermark <0-100>|idle-radio-send-multicast [enable]|
  legacy-load-balance|map-radios <1-127>|radio-mic-cfg <LINE>|rate-scale|
  request-ap-log <1-1024>|rogue-find-range <1-10>|save-ap-log|
  snmp-trap-throttle <1-20>|sync-radio-entries|vlan-cache [enable]]
```

Parameters

service (clear)	
clear [wireless] [mobile-unit] [association-statistics]	Clears wireless mobile unit associations and reassociation statistics. • wireless – Wireless parameters • mobile-unit – Mobile-unit parameters • association-history – Clears association and reassociation statistics

service (show)	

show [cli|radio-neighbor|smart-rf|wireless]	Shows current running system information.
	• cli – Shows the CLI tree of the current mode
	• radio-neighbor [mu <MAC-ADDRESS>] –Shows neighboring radios for a station.
	  • mu <MAC-ADDRESS> – Specify the MAC address of the MU in the AA-BB-CC-DD-EE-FF format.
	• smart-rf [debug-config|sensitivity] – Shows Smart-RF manangement commands.
	  • debug-config – Displays Smart-RF debug configuration.
	  • sensitivity [mu|pattern|rates] – Displays Smart-RF sensitivity table.
	  • mu {<1-8192> <WORD>}– Optional. Displays the Smart-RF sensitivity table for a specified MU. You can specify the MU using one of the following options:
	  • <1-8192> – Optional. The MU index between 1 - 8192.
	  • <MAC-ADDRESS> – Optional. The MAC address of MU cache entry to show.
	  • pattern [pattern-11a|pattern-11b|pattern-11bg|patter-2-mbps] – Displays Smart-RF sensitivity table for a common MU pattern. The patterns are as follows:
	  • pattern-11a – 11a unit
	  • pattern-11b – 11b unit
	  • pattern-11bg – 11bg unit
	  • pattern-2-mbps – 2Mbps units
	  • rates <RATE-FLAGS> – Displays sensitivity table for a common mu pattern. Specify the rate-flags in hexadecimal format.
	• wireless – Displays Wireless parameters configured. Select one of the following options to view the configured values:
	  • ap-history, buffer-counters, enhanced-beacon-table, enhanced-probe-table, group, group-stats, legacy-load-balance, mu-cache-buckets, mu-cache-entry, mv-lan, radio, radio-cache-entry, radio-hash-buckets, snmp-trap-throttle, vlan-cache-buckets, vlan-cache-entry, waiting.

service (show) wireless	
ap-history <XX-XX-XX-XX-XX-XX>	Displays access port serviceability parameters. Use history to access port history. The following options can be used to access AP history: • <XX-XX-XX-XX-XX-XX> – Optional. The access port MAC address.
buffer-counters	Displays allocation counts for various buffers.

enhanced-beacon-table [config|report]	Displays the following enhanced beacon tables for AP locationing: • config – Enhanced beacon table for AP locationing configuration parameters. • report – Enhanced beacon table for AP locationing report.
enhanced-probe-table [config|report]	Displays the following enhanced beacon tables for MU locationing: • config – Enhanced beacon table for MU locationing configuration parameters. • report – Enhanced beacon table for MU locationing report.
group <1-256>	Displays radio group related debug information. Specify the index in the range <1-256>
group-stats	Displays radio group statistics information.
legacy-load-balance	Displays legacy load balance algorithm compatibility mode.
mu-cache-buckets	Displays Wireless mobile units cache buckets.
mu-cache-entry {<1-8192>| <MAC-ADDRESS>}	Displays MU cache information based on the parameters passed (dumps whole table if no parameters passed). • <1-8192> – Optional. Provide a single index • <MAC-ADDRESS> – Optional. Provide MAC address of MU cache entry.
mvlan <1-256>	Displays Multi-Vlan debug statistics. • <1-256> – Specify the WLAN index.
radio {<1-4096>|description| mapping}	Displays radio serviceability parameters based on the option selected. • <1-4096> – Optional. Provide a single radio index. • description – Optional. Displays description and location co-ordinates of radios. • mapping – Optional. Displays radio to CPU mapping.
radio-cache-entry {<MAC-ADDRES>}	Displays radio cache information. • <MAC-ADDRESS> – Optional. Specify the MAC address of the radio cache entry.
radio-hash-buckets	Displays Wireless radio hash buckets.
vlan-cache-buckets	Displays Wireless VLAN cache buckets.
vlan-cache-entry {<1-8192>| <MAC-ADDRESS>}	Displays mu vlan cache information • <1-8192> – Optional. Provide a single index. • <MAC-ADDRESS> – Optional. Provide the MU MAC address of VLAN cache entry to show.
waiting {<0-99>}	Displays waiting table of contents. • <0-99> – Optional. Specify the index in the wait table in the range <0-99>.
service (smart-rf)	
clear-history	Clears assignment history
load-from-file	Loads Smart-RF configuration from the smart.bin file.

replay [enable]	Enables Smart-RF replay mode.
rescue <MAC-ADDRESS>	Forces radio rescue operation. • <MAC_ADDRESS> – A single radio's MAC address, a single radio index, or a list of radio indices.
restore <MAC-ADDRESS>	Restores any recovering operation on given radio. • <MAC_ADDRESS> – A single radio's MAC address, a single radio index, or a list of radio indices.
save-to-file	Saves Smart-RF records to smart.bin file
simulate [coverage-hole| interference]	Simulates radio events • coverage-hole <1-4096> UNIT_RANGE – simulates coverage hole event on the specified radio. Specify the radio using one of the following options: • <1-4096> – Provides a single radio's index • UNIT_RANGE – Provides the experienced rate in Mbps. • interference – Simulates interference on a specified radio. • <WORD> – A single radio's MAC address, a single radio index, or a list of radio-indices.
service (wireless)	
ap-history [clear|enable]	Configures the following access port serviceability parameters: • clear – Deletes all AP history. • enable – Enables the tracking of AP history.
clear-ap-log <1-1024>	Clears access port logs for the selected access port index. Select an access port index between 1 - 1024.

custom-cli [sh-wi-mobile-unit [ap-loan| ap-name|channel| dot11-type|ip| last-heard|mac| radio-bss|radio-desc| radio-id| ssid|state|username| vlan|wlan|wlan-id]| sh-wi-radio [adopt-info|ap-locn| ap-mac| ap-name|channel| dot11-type| mum-mu|power| pref-id|radio-bss| radio-desc|radio-id|state]	Customizes the output of some summary Wireless CLI commands. • sh-wi-mobile-unit – Customizes the output of the `show wireless mobile-unit` command. • ap-locn – Specifies the location of the AP where the MU is associated. • ap-name – Specifies the name of the AP where the MU is associated. • channel – Specifies the channel of the radio where the MU is associated. • dot11- type – Specifies the dot11 radio type of the MU. • ip – Specifies the IP address of the MU. • last-heard – Specifies the time when a packet was last received from the MU. • mac – Specifies the MAC address of MU. • radio-bss – Specifies the radio's BSSID where the MU is associated. • radio-desc – Specifies the radio's description the MU is associated. • radio-id – Specifies the radio's index to which the MU is associated. • ssid – Specifies the MU WLAN's SSID. • state – Specifies the current state of the MU. • username – Species the RADIUS username of the user connected through this device. • vlan – Specifies the VLAN ID assigned to the MU. • wlan – Specifies the WLAN description the MU is using. • wlan-id – Specifies the WLAN index the MU is using.
	• sh-wi-radio – Customizes the output of the `show wireless radio` command. • adopt-info – Specifies radio adoption information (whether the radio is on the current switch or some other switch in the cluster) • ap-locn – Specifies the location of the AP to which this radio belongs. • ap-mac – Specifies the MAC address of AP to which the radio belongs. • ap-name – Specifies the name of the AP to which this radio belongs. • channel – Specifies the radio's configured and current channel. • dot11-type – Specifies the radio's dot11 type (11a/11g etc). • num-mu – Specifies the number of mobile devices associated with this radio. • power – Specifies the radio's configured and current transmit power.pref-id – Specifies the radio's adoption preference ID. • radio-bss – Specifies the radio's BSSID.radio-desc – Specifies the radio's description. • radio-id – Specifies the radio index in configuration. • state – Specifies the radio's current operational state.

dot11i enforce [pmkid-validation]	Modifies dot11i service parameters. • enforce – Modifies enforcement of various dot11i validations. • pmkid-validation – Toggles PMKID validation in dot11i handshake message from client.

enhanced-beacon-table [channel-set|enable| erase-report|max-ap| scan-interval|scan-time]	Configures enhanced beacon table for AP locationing.
	• channel-set – Sets channel set for enhanced beacon table. The options are:
	  • a <1-200> – Adds channels to channel set for enhanced beacon table for 802.11a radios.
	  • an <1-200> – Adds channels to channel set for enhanced beacon table for 802.11an radios.
	  • bg <1-200> – Adds channels to channel set for enhanced beacon table for 802.11bg radios.
	  • bgn <1-200> – Adds channels to channel set for enhanced beacon table for 802.11bgn radios.
	  • <1-200 > – List of space separated channel number(s) between 1 - 200.
	• enable – Enables enhanced beacon table for AP locationing.
	• erase-report – Erases the enhanced beacon table for AP locationing report.
	• max-ap <0-512> – Sets the maximum number of APs in the enhanced beacon table for AP locationing.
	• scan-interval <10-60> – Sets the time duration, in seconds, between two enhanced beacon table for AP locationing scans.scan-time <100-1000> – Sets the time duration, in milliseconds, of an enhanced beacon table scan.

enhanced-probe-table [enable|erase-report| max-mu|preferred| window-time]	Configures enhanced probed table for MU locationing. • enable – Enables enhanced probe table for MU locationing. • erase-report – Erases the enhanced probe table for MU locationing report. • max-mu <0-512> – Maximum number of MUs in the report • preffered <XX-XX-XX-XX-XX-XX> – Adds the given MAC address to the preferred MU list. Specify the MAC address in AA-BB-CC-DD-EE-FF format. • window-time <10-60> – Sets the window time, in seconds, for probe collection.
forward-eap-to-wired	Forwards EAP packets from a MU to the wired side for the wired switch to perform 802.1x authentication. **Note:** Does not apply for EAP frames directed to the BSS for wireless 802.1x EAP Authentication.
free-packet-watermark <0-100>	Sets the free packets threshold.The watermark percentage range is <0-100>. If the percentage of free packets is lower than this number, additional packets will not be queued up in the datapath.

idle-radio-send-multicast [enable]	Forwards multicast packets to radios without associated MUs. • enable – Enables multicast forwarding
legacy-load-balance	Invokes legacy load balance algorithm with RFS7000 wireless controller.
map-radios <1-127>	Sets radio to CPU mapping constants. • <1-127> – Specify the radio to CPU mapping constant between 1 -127.
radio-mic-cfg <LINE>	Sets the radio specific miscellaneous configuration – U16 for all radios.
rate-scale	Enables wireless rate scaling (this feature is enabled by default).
request-ap-log <1-1024>	Requests an access port log for the selected access port. Select an access port index between 1 - 1024.
rogue-find-range <1-10>	Sets rogue search range (<1-10> is the numeric range).
save-ap-log	Saves debug/error logs sent by the access port.
snmp-trap-throttle <1-20>	Limits the number of SNMP traps generated from the wireless module between 1 - 20.
sync-radio-entries	Synchronizes radio configuration entries at cluster level.
vlan-cache [enable]	Enables the VLAN cache mode. • enable – Enables default setting

Example

```
RFS7000(config-wireless)#service show cli | include LI
          +-LINE [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
          +-any [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
          +-LINE [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
          +-any [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
  +-LINE [do LINE]
      +-<1-200> [no ap-detection approved (<1-200>|IDX-LIST)]
      +-IDX-LIST [no ap-detection approved (<1-200>|IDX-LIST)]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
          +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
          +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
      +-LINE [radio <1-4096> description LINE].................

RFS7000(config-wireless)#service show wireless buffer-counters
wispe alloc: 7
wispe free : 7
mu alloc   : 0
mu free    : 0
RFS7000(config-wireless)#

RFS7000(config-wireless)#service wireless save-ap-log
RFS7000(config-wireless)#

RFS7000(config-wireless)#service enhanced-beacon-table channel-set a 44 52
RFS7000(config-wireless)#
```

20.1.45 smart-rf

Wireless Configuration Commands

Use this command to configure Smart-RF management parameters, and move to the (`config-wireless-smart-rf`) instance.

Syntax

```
smart-rf
```

Parameters

None.

Example

```
RFS7000(config-wireless)#smart-rf
RFS7000(config-wireless-smart-rf)#
```

20.1.46 show

Wireless Configuration Commands

Use this command to view current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFS7000(config-wireless)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
```

```
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-wireless)#
```

20.1.47 smart-scan-channels

Wireless Configuration Commands

Use this command to revert smart scan channels to default.

Syntax

Parameters `smart-scan-channel [<CHANNEL-LIST>|add <CHANNEL-LIST>|remove <CHANNEL-LIST>]`

<CHANNLE-LIST>	Specifies a comma-separated list of channels.
add <CHANNLE-LIST>	Adds one or more channels to the existing channel list.
remove <CHANNLE-LIST>	Removes one or more channels from the existing channel list.

Example

```
RFS7000(config-wireless)#smart-scan-channels add AAA-ABB-CC-KK-SS
RFS7000(config-wireless)#
```

20.1.48 test

Wireless Configuration Commands

Use this command to test neighbor report on air.

Syntax

```
test dot11k [make-bcn-rep|send-beacon-req|send-nbr-rep]

test dot11k make-bcdn-rep [mu <MAC-ADDRESS>] [neighbor <MAC-ADDRESS>]

test dot11k send-beacon-request [<1-8192>|MU <LIST>|mu <MAC-ADDRESS>]
  {measurement-duration <100-10000>}

test dot11k send-nbr-rep [mu <MAC-ADDRESS>]
```

Parameters

dot11k	Invokes dot11k related commands.
make-bcn-rep [mu <MAC-ADDRES>] [neighbor <MAC-ADDRESS>]	Makes beacon report • mu <MAC-ADDRESS> – Specifies the MU's MAC address in the AA-BB-CC-DD-EE-FF format. • neighbor <MAC-ADDRESS> – Specifies the neighboring radio's MAC address in the AA-BB-CC-DD-EE-FF format.
send-beacon-request [<1-8192>| MU <LIST>| mu <MAC-ADDRESS>]	Triggers the beacon request send action. • <1-8192> – Specifies a single MU index. • MU <LIST> – Specifies a list (for example, 1,3,7) or a range (for example, 1-7) of MU indices. • mu <MAC-ADDRESS> – Specifies MU's MAC address. • measurement-duration <100-10000> – Optional. Specifies measurement duration in TUs between 100 - 10000.
send-nbr-req [mu <MAC-ADDRES>]	Triggers the neighbor report send action. • mu <MAC-ADDRESS> – Specifies the MU's MAC address in the AA-BB-CC-DD-EE-FF format.

Example

```
RFS7000(config-wireless)#test dot11k send-nbr-rep mu 11-22-33-44-55-66
% Error: MU is not present
RFS7000(config-wireless)#
```

20.1.49 wips

Wireless Configuration Commands

Use this command to configure WIPS parameters.

Syntax

```
wips [detect-window|disable|event|reset-to-default]
wips detect-window <5-300>

wips event [80211-replay-check-failure|ad-hoc-advertising-authorized-ssid|
ad-hoc-network-violation-authorized-device|
ad-hoc-network-violation-unauthorized-device|aggressive-scanning|all|
ap-default-configuration|ap-ssid-broadcast-in-beacon|
crackable-wep-iv-key-used|decryption-failures|
dos-association-or-authentication-flood|
dos-broadcast-deauthentication|dos-eapol-start-storm|
dos-unicast-deauthentication-or-disassociation|eap-flood|eap-nak-flood|
failures-reported-by-authentication-servers|fake-ap-flood|
frames-from-unassociated-stations|frames-with-bad-essids|
fuzzing-all-zero-mac-address-observed|fuzzing-invalid-frame-type-detected|
fuzzing-invalid-management-frame|fuzzing-invalid-sequence-number|
identical-source-and-destination-addresses|impersonation-attack-detected|
invalid-8021x-frames|non-changing-wep-iv|replay-injection-attack|
suspicious-ap-high-rssi|transmitting-device-using-invalid-mac|unencrypted-station-
transmission-detected]
```

Parameters

detect-window <5-300>	Sets the number of seconds for which information is collected before analysis. All thresholds are functions of this window size.
disable	Disables WIPS without affecting the configuration.

event [80211-replay-check-failure| ad-hoc-advertising-authorized-ssid | ad-hoc-network-violation-authorized-device| ad-hoc-network-violation-unauthorized-device|aggressive-scanning|all| ap-default-configuration| ap-ssid-broadcast-in-beacon|crackable-wep-iv-key-used |decryption-failures| dos-association-or-authentication-flood| dos-broadcast-deauthentication| dos-eapol-start-storm| dos-unicast-deauthentication-or-disassociation|eap-flood|eap-nak-flood| failures-reported-by-authentication-servers|fake-ap-flood|frames-from-unassociated-stations|frames-with-bad-essids|fuzzing-all-zero-mac-address-observed|fuzzing-invalid-frame-type-detected|	Configures WIPS event monitoring. The events are:
	• 80211-replay-check-failure [enable {authorized|ignored|unauthorized}| filter-out <1-86400>|threshold [mu|radio]] – 802.11 replay check failure settings.
	  • enables – Enables monitoring, filtering, and triggering alarms.
	  • filter-out <1-86400> – Filters the MU's age-out limit.
	  • threshold [mu|radio] – Configures the threshold for events allowed in the detection window. This threshold is used to monitor on a per-MU/ per-radio basis.
	• ad-hoc-advertising-authorized-ssid [enable|filter-ageout <1-806400>] – Monitors ad-hoc advertising events.
	• ad-hoc-network-violation-authorized-device [enable [authorized|ignored| unauthorized]|filter-ageout <1-806400>] – Monitors ad-hoc network violation for authorized devices.
	• ad-hoc-network-violation-unauthorized-device [enable [authorized| ignored|unauthorized]|filter-ageout <1-806400>] – Monitors ad-hoc network violation for unauthorized devices.
	• aggressive-scanning [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors aggressive scanning events.
	• all [filter-ageout <1-86400>] – Monitors all events.
	• ap-default-configuration enable [authorized|ignored|unauthorized] – Monitors triggers against authorized/ignored/unauthorized AP default configuration.
	• ap-ssid-broadcast-in-beacon enable [authorized|ignored|unauthorized] – Monitors AP SSID broadcast in beacon events.
	• crackable-wep-iv-key-used [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>] – Monitors crackable WEP IV Key used events.
	• decryption-failures [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors decryption failures.
	• dos-association-or-authentication-flood [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors DoS association or authentication flood events.
	• dos-broadcast-deauthentication [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors DOS broadcast deauthentication events.
	• dos-eapol-start-storm [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors DoS EAPOL-Start Storms.
	• dos-unicast-deauthentication-or-disassociation [enable [authorized|ignored|unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors DoS unicast deauthentication or disassociation events.

fuzzing-invalid-management-frame| fuzzing-invalid-sequence-number|identical-source-and-destination-addresses| impersonation-attack-detected|invalid-8021x-frames| non-changing-wep-iv|replay-injection-attack|transmitting-device-using-invalid-mac| unauthorized-ap-using-authorized-ssid |unencrypted-station-transmission-detected]	• eap-flood eap-flood [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors EAP flood events. • eap-nak-flood [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors EAP-NAK flood – EAP flood events. • failures-reported-by-authentication-servers [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors failures reported by authentication servers. • fake-ap-flood [enable [authorized|ignored|unauthorized]| filter-ageout <1-86400>|threshold [mu|radio]] – Monitors fake AP flood (based on number of APs observed in a minute). • frames-from-unassociated-stations [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors frames from unassociated stations. • frames-with-bad-essids [<1-10> <STRING> |enable [authorized|ignored|unauthorized]|filter-ageout <1-86400>] – Monitors frames with bad ESSIDs. • fuzzing-all-zero-mac-address-observed [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors fuzzing: all zero MAC address observed. • fuzzing-invalid-frame-type-detected [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors fuzzing: Invalid Frame Type Detected. • fuzzing-invalid-management-frame [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors fuzzing: Invalid Management Frame. • fuzzing-invalid-sequence-number [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors Fuzzing: Invalid Sequence Number. • identical-source-and-destination-addresses [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors identical source and destination addresses • impersonation-attack-detected [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors impersonation attack detected. • invalid-8021x-frames [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>] – Monitors invalid 802.1X frames • non-changing-wep-iv [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400] – Monitors non-changing WEP IV events. • replay-injection-attack [enable [authorized|ignored| unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors replay injection attacks. • suspicious-ap-high-rssi [signal-strength-threshold <-100-0>|enable [authorized|ignored|unauthorized]|filter-ageout <1-86400>] – Monitors suspicious AP - High RSS.

	• transmitting-device-using-invalid-mac [enable [authorized|ignored|unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors Transmitting Device Using Invalid MAC events.
	• unauthorized-ap-using-authorized-ssid [enable [authorized|ignored|unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors unauthorized AP using authorized SSID events.
	• unencrypted-station-transmission-detected [enable [authorized|ignored|unauthorized]|filter-ageout <1-86400>|threshold [mu|radio]] – Monitors unencrypted station transmission detected events.
	  • enable [authorized|ignored|unauthorized] – Enables monitoring, filtering and triggering alarms.
	  • authorized – Triggers against authorized devices.
	  • ignored – Triggers against ignored devices.
	  • unauthorized – Triggers against unauthorized devices.
	  • filter-out <1-86400> – Filters age-out duration for the mobile unit.The duration ranges from 1- 86400 seconds
	  • threshold <mu|radio> – Configures the threshold of events allowed in the detection window.
	  • mu <0-65535> – Uses the threshold for monitoring on a per-mobile-unit basis.
	  • radio <0-65535> – Uses the threshold for monitoring on a per-radio basis.
	  • <0-65535> – The threshold of events allowed in the detection window.

reset-to-default	Resets to default settings.

Example

```
RFS7000(config-wireless)#wips detect-window 5
RFS7000(config-wireless)#

RFS7000(config-wireless)#wips event 80211-replay-check-failure filter-ageout 2
RFS7000(config-wireless)#

RFS7000(config-wireless)#wips reset-to-default
RFS7000(config-wireless)#
```

20.1.50 wlan

Wireless Configuration Commands

Use this command to configure Wireless LAN parameters.

Syntax

```
wlan [<1-256>|<WLAN-LIST>] [80211-extensions|802.11w-pmf|aap-proxy-radius|
  accounting|acl|add-vlan|answer-bcast-ess|authentication-type|client-bridge-backhaul|
  deny-static-mu|description <LINE>|dot11i|enable|encryption-type [hold-time <1-
300>|hotspot|inactivity-timeout <60-86400>|independent|ip|
  max-flows-per-mu|mobility [enable]|mu-mu-disallow|nac-mode|nas-id <NAS-ID>|
  nas-port-id <NAS-PORT-ID>|qos|radius|secure-beacon|set-vlan-user-limit|
  smart-scan-channels|ssid <WLAN-SSID>|storm-control|syslog|url-log [enable]|vlan]

wlan [<1-256>|<WLAN-LIST>] 80211-extensions move-command enable

wlan [<1-256>|<WLAN-LIST>] 80211w-pmf [optional|requires|sa-query (max-timeout|
  retry-timeout)]
wlan [<1-256>|<WLAN-LIST>] aap-proxy-radius enable {realm <REALM-NAME>} {strip}}

wlan [<1-256>|<WLAN-LIST>] acl exceed-rate [mu-denied-traffic <0-1000000>]
{disassociate}

wlan [<1-256>|<WLAN-LIST>] accounting [none|radius|ssyslog)]
wlan [<1-256>|<WLAN-LIST>] add-vlan [<1-4094>|<VLAN-LIST>] {limit <0-8192>}

wlan [<1-256>|<WLAN-LIST>] authentication-type [eap|hotspot]

wlan [<1-256>|<WLAN-LIST>]client-bridge-backhaul [enable]

wlan [<1-256>|<WLAN-LIST>] dot11i [handshake|key|key-rotation [enable]|
  key-rotation-interval <30-86400>|opp-pmk-caching|pmk-caching|preauthentication|
  second-key]
wlan <[1-256>|<WLAN-LIST>] dot11i handshake [timeout <100-5000>] [retransmit <1-10>]
wlan [<1-256>|<WLAN-LIST>] dot11i key [0 <WORD>|2 <WORD>|<WORD>]
wlan [<1-256>|<WLAN-LIST>] dot11i second-key [enable|key [0 <WORD>|2 <WORD>|<WORD>]]
wlan [<1-256>|<WLAN-LIST>] hotspot [allow-eap|allow-list|cache-ageout <5-86400>|
  connection-mode [https]|ntf-logout-port <0-65535>|query|redirect-to-hostname|
  simultaneous-users <0-8192>|webpage|
  webpage-location)
wlan [<1-256>|<WLAN-LIST>] hotspot allow-list <1-32> <IP-ADDRESS>
wlan [<1-256>|<WLAN-LIST>] hotspot query [<1-10>|<QUERY>]
wlan [<1-256>|<WLAN-LIST>] hotspot webpage [external|internal] [failure|login|welcome]
wlan [<1-256>|<WLAN-LIST>] hotspot webpage-location [advanced|external|internal
  {logout-on-browser-close}]

wlan [<1-256> ip [arp [rate-limit|trust]|dhcp [trust]]

wlan [<1-256>nac-mode [bypass-nac-except-include-list|bypass-nac-except-exclude-list|
  none]

wlan [<1-256>|<WLAN-LIST>] qos [classification|mcast-with-dot11i [enable]|
  mcast1 <MAC-ADDRESS>|mcast2 <MAC-ADDRESS>|prioritize-voice|rate-limit|
  svp [enable]|weight <1-10>|wmm)

wlan [<1-256>|<WLAN-LIST>] qos classification [low|normal|video|voice|wmm]
wlan [<1-256>|<WLAN-LIST>] qos rate-limit [wired-to-wireless|wireless-to-wired]
  <100-1000000>
wlan [<1-256>|<WLAN-LIST>] qos wmm [8021p|background|best-effort|dscp|video|voice)
  (aifsn|cw|txop-limit|)

wlan [<1-256>|<WLAN-LIST>] radius [accounting|authentication-protocol|dscp <0-63>|
  dynamic-authorization [enable]|dynamic-vlan-assignment [enable]|
  mobile-unit|reauth <30-65535>|server]

wlan [<1-256>|<WLAN-LIST>] radius accounting [mode|server|timeout]
wlan [<1-256>|<WLAN-LIST>] radius accounting mode [start-interim-stop [interval
  <60-3600>]|start-stop|stop-only]
wlan [<1-256>|<WLAN-LIST>] radius accounting server [primary|secondary]
  [<A.B.C.D>|radius-key [0 [<WORD>|2 <WORD>|0 <WORD>]]
```

```
wlan [<1-256>|<WLAN-LIST>] radius accounting timeout <1-300> [retransmit <1-100>]

wlan [<1-256>|<WLAN-LIST>] radius authentication-protocol [chap|pap]
wlan [<1-256>|<WLAN-LIST>] radius mobile-unit [time-out <1-300>] [retransmit <1-100>]
wlan [<1-256>|<WLAN-LIST>] radius server [primary|secondary|timeout]
wlan [<1-256>|<WLAN-LIST>] radius server [primary|secondary] [<A.B.C.D>|radius-key
  [0 <WORD>|2 <WORD>|<WORD>]]
wlan [<1-256>|<WLAN-LIST>] radius server timeout <1-300> [retransmit <1-100>]

wlan [<1-256>|<WLAN-LIST>] smart-scan-channels [<CHANNEL-LIST>|add <CHANNEL-LIST>|
  remove <CHANNEL-LIST>]
wlan [<1-256>|<WLAN-LIST>] set-vlan-user-limit [<1-4094>|<VLAN-LIST>]

wlan [<1-256>|<WLAN-LIST>] storm-control [bcast|mcast|ucast] [rate-limit <1-1000000>]

wlan [<1-256>|<WLAN-LIST>] syslog accounting server <IP-ADDRESS>

wlan [<1-256>|<WLAN-LIST>] vlan [<1-4094>|<VLAN-LIST>] {limit <0-8192>}
```

Parameters

[<1-256>|<WLAN-LIST>]	Select a single WLAN index. You also have the option of selecting a list (1,3,7) or range (3-7) of WLAN indices.
80211-extensions (move-command) (enable)	Enables support for extensions to 802.11. • move-command – Enables support for the move-command (fast roaming). • enable – Enables the 802.11 extension.

80211w-pmf [optional|required|sa-query]	Sets the following 802.11w *protected management frames* (pmf):
	• optional – *Management Frame Protection* (MFP) optional.
	• required – MFP required
	• sa-query [max-timeout <100-6000>|retry-timeout <10-1500>] – SA Query Protocol settings.
	  • max-time <100-6000> – Sets the maximum timeout in milliseconds.
	  • retry-timeout <10-1500> – Sets the retry timeout in milliseconds.

aap-proxy-radius (enable)	Configures proxying AAP RADIUS requests.
	• enable {realm <REALM-NAME>} {strip} – Enables proxying AAP RADIUS requests.
	  • realm <REALM-NAME> – Optional. Specify the realm name.
	  • strip – Optional. Strips realm name while proxying requests.

accounting (none|radius|syslog)	Configures WLAN accounting parameters. • none – No accounting on this WLAN. • radius – Uses RADIUS accounting on this WLAN. • syslog – Uses syslog accounting on this WLAN.

acl (exceed-rate) (mu-denied-traffic) <0-1000000> (disassociate)	Configures the actions taken based on ACL configuration (including packet drop).
	• exceed-rate – Sets the actions taken when a rate is exceeded.
	  • mu-denied-traffic – The action is to deny traffic from the MU.
	  • <0-1000000> – Allowed rate threshold of disallowed MU traffic in packets/sec
	  • disassociate – Optional. Enables/disables disassociate. When enabled, disassociates the MU.

add-vlan [<1-4094>|<VLAN-LIST>] {limit <0-8192>}	Instead of starting a new VLAN assignment for the given WLAN, this command adds a VLAN assignment to the existing VLAN assignment. All prior VLAN settings will be retained. • [<1-4094>|<VLAN-LIST>] – Sets the VLAN range list. It can be either a single index or a list (for example,1,3,7) or range (for example, 3-7) of indices. • limit <0-8192> – Optional. Sets user limits on VLANs for this WLAN. **Note:** The `[no]` form of `add-vlan` command will delete the specified VLAN mapping, iterating over the specified WLAN range list. If the specified VLAN mapping does not exist for particular WLAN, a warning "specified VLAN does not exists" displays. The delete action continues on the remaining VLANs. If all VLANs are deleted. A default VLAN assignment occurs.
answer-bcast-ess	Allows this WLAN to respond to probes for broadcast ESS.
authentication-type (eap|hotspot)	Sets the authentication type of this WLAN. • eap – EAP authentication (802.1X) • hotspot – Web-based authentication
client-bridge-backhaul (enable)	Client bridge backhaul capability on this WLAN. • enable – Enables this capability
deny-static-mu	Drop packets from static MUs.
description <LINE>	Sets the WLAN's description (used to identify the WLAN).

dot11i [handshake|key| key-rotation|ey-rotation-interval| opp-pmk-caching| pmk-caching| preauthentication| second-key]	Modifies related parameters.
	• handshake [timeout <100-5000>] [retransmit <1-10>] – Uses a AES handshake to configure timeout and retransmission parameters.
	  • timeout <100-5000> – The timeout (in milliseconds) between retries.
	  • retransmit <1-10> – The number of retransmission attempts.
	• key [0 <WORD>|2 <WORD>|<WORD>] – Configure the key (PMK)
	  • 0 <WORD> – Password is specified UNENCRYPTED
	  • 2 <WORD> – Password is encrypted with password-encryption secret
	  • <WORD> – The 256bit (64 hex characters) long key
	• key-rotation (enable) – Controls the periodic update of the broadcast keys for associated MUs.
	• key-rotation-interval <30-86400> – Configures the broadcast key rotation interval between 30 - 86400 seconds.
	• opp-pmk-caching – Enables the opportunistic use of cached pairwise master keys (fast roaming with EAP/802.1X).
	• pmk-caching – Enables the use of cached pairwise master keys for fast roaming with eap/802.1X.
	• preauthentication – Enables support for 802.11i pre-authentication.
	• second-key [enable|key] [0 <WORD>|2 <WORD>|<WORD>] – Configures a secondary set of key/passphrase for this WLAN.
	  • enable – Enables the use of a secondary key/passphrase.
	  • key – Configures the key (PMK).
	  • 0 <WORD> – Password is specified UNENCRYPTED.
	  • 2 <WORD> – Password is encrypted with password-encryption secret.
	  • <WORD> – The 256bit (64 hex characters) long key.

enable	Enables the specified Wireless LAN(s)
hold-time <1-300>	Sets the time duration, in seconds, to hold user credentials when a MU leaves or roams.

hotspot [allow-eap|allow-list| cache-ageout| connection-mode| ntf-logout-port|query| redirect-to-hostname| simultaneous-users| webpage| webpage-location]	Modifies hotspot related parameters
	• allow-eap – Allows EAP authentication in addition to Web-based login.
	• allow-list <1-32> <IP-ADDRESS> – Modifies hotspot allow-list parameters. Users who have not yet authenticated are allowed access to these IP addresses. Typically this would be the external Web page IP addresses.
	  • <1-32> – The allow list rule index between 1 -23.
	  • IP address – The allow list IP address. This parameter specifies IP addresses to which unauthenticated MUs can connect to. It does not specify a network or subnet.
	• cache-ageout <5-86400> – Configures hotspot cache ageout
	  • <5-86400> – Time in seconds to age out the cache after MU disassociation.
	• connection-mode [https] – Sets the connection mode type as HTTPS.
	• ntf-logout-port – Configures port to send NTF-Logout in Web-portal mode hotspot.
	  • <0-65535> – Select a port between 1 - 65535, or 0 to use original source port in req-challenge.
	  • query [<1-10> |<QUERY-LIST>] – Specifies queries to be appended to the redirection URL.<1-10> – Provide a single index.
	  • <QUERY-LIST> – Provide a list (for example, 1,3,7) or range (for example, 3-7) of indices.
	• redirect-to-hostname – Uses the wireless controller's hostname/system-name in the redirection URL instead of the IP address.
	• simultaneous-users <0-8192> – Enforces that a particular username can only be used by certain number of MAC addresses at a time.
	  • <0-8192> –The number of MAC addresses that are allowed to use that username at the same time. 0 implies disabling of the checks.

	• webpage (external|internal) (failure|login|welcome) – Modifies hotspot page parameters.
	  • external – Modifies a hotspot's external page.
	  • internal – Modifies hotspot's internal page.
	  • failure – Users are redirected to this Web page if they fail authentication.
	  • login – Users are prompted for their username and password within this Web page.
	  • welcome – Users are redirected to this Web page after they authenticate successfully.
	• webpage-location (advanced|external|internal) – The location of the Web pages used for authentication. These pages can either be hosted on the switch or an external Web server.

	• advanced – Uses login/welcome/failure Web pages created by the user on the switch. • external – Uses login/welcome/failure Web pages on an external server. • internal – Uses login/welcome/failure Web pages created automatically on the switch.
inactivity-timeout <60-86400>	Sets the inactivity timeout in seconds. If a frame is not received from a mobile unit for this interval, the mobile unit is disassociated.
independent	Sets this WLAN as an independent WLAN.

ip [arp|dhcp]	Sets Internet Protocol parameters for *Address Resolution Protocol* (ARP) and DHCP packets.
	• arp [rate-limit|trust] – Sets ARP parameters
	• dhcp [trust] – Sets DHCP parameters.
	  • rate-limit <1-1000000> – Rate limits ARP packet between 1 - 1000000 packets/sec.
	  • trust – Sets the ARP/DHCP responses as trusted for this WLAN/range of WLANs.

max-flows-per-mu <1-10000>	Sets the maximum firewall flows per mobile-unit between 1 -10000.
mobility (enable)	Enables L3 Mobility on WLAN(s).
mu-mu-disallow	Disallows frames from one MU to another MU on this WLAN.
nas-id <NAS-ID>	Sets the NAS ID of this WLAN to send to RADIUS server. • <NAS-ID> – A string of up to 256 characters in length.
nas-port-id <NAS-PORT-ID>	Sets the NAS PORT ID of this WLAN to send to RADIUS server. • <NAS-PORT-ID> – A string of up to 256 characters in length.

qos [classification| mcast-with-dot11i| mcast1|mcast2| prioritize-voice| rate-limit|svp| weight|wmm]	Sets *Quality of Service* (QoS) parameters.
	• classification [low|normal|video|voice|wmm] – Specifies how traffic on this WLAN is classified (relative prioritization on the access port). The options are:
	  • low – Traffic on this WLAN is treated as low priority (background).
	  • normal – Traffic on this WLAN is treated as normal priority (best-effort).
	  • video – Traffic on this WLAN is treated as video.
	  • voice – Traffic on this WLAN is treated as voice.
	  • wmm – Uses WMM-based classification (using DSCP or 802.1p tags) to classify traffic into different queues.
	• mcast-with-dot11i (enable) – Enables multicast mask with dot11i.
	• [mcast1|mcast2] <AA-BB-CC-DD-EE-FF> – Sets the Egress prioritization multicast mask.
	  • <AA-BB-CC-DD-EE-FF> – The MAC address in AA-BB-CC-DD-EE-FF format.
	• prioritize-voice – Prioritizes voice frames over general data frames (applies non-WMM mobile unit).
	• rate-limit [wired-to-wireless|wireless-to-wired] <100-1000000> – Sets traffic rate limit for users on specified WLAN(s).
	  • wired-to-wireless – Down link direction - from network to wireless client.
	  • wireless-to-wired – Up link direction - from wireless client to network.
	  • <100-1000000> – Rate in the range of <100-1000000> kbps.
	• svp (enable) – Enables *Spectralink Voice Prioritization* (SVP) support on this WLAN.
	• weight <1-10> – Sets the Egress weight (relative priority to other WLANs) of this WLAN. Specify a value between 1 - 10.
	• wmm [8021p|background|best-effort|dscp|video|voice] (aifsn|cw|txop-limit| acm) – Sets the 802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300).
	  • 8021p – Uses 802.1p frame priority (field in the VLAN tag) to determine packet priority.
	  • background – Sets background category traffic parameters.
	  • best-effort – Sets best effort category traffic parameters.
	  • dscp – Uses *Differentiated Services Code Point* (DSCP) bits in the IP header to determine packet priority.
	  • video – Sets video category traffic parameters.
	  • voice – Sets voice category traffic parameters.

	• aifsn <2-15> – *Arbitration Inter Frame Spacing Number* (AIFSN) is the wait time (in milliseconds) between data frames derived using AIFSN and the slot-time. •<2-15> – The AIFSN spacing number. • cw <0-15> <0-15> – *Contention Window* (CW) parameters. MU's pick a number between 0 and the minimum contention window to wait before retrying transmissions. MU's double their wait time on a collision, until they reach the maximum contention window. •<0-15> – The CW minimum value (the actual value used is 2^ECWmin - 1). •<0-15> – The CW maximum value (2^ECWmax - 1). • txop-limit <0-65535> – (Transmit-opportunity): An interval when a particular WMM STA has the right to initiate transmissions on the wireless medium. •<0-65535> – The transmit opportunity in 32 microsecond units.

radius [accounting| authentication-protocol| dscp| dynamic-authorization| dynamic-vlan-assignment| mac-auth-format| mobile-unit| reauth| server]	Configures RADIUS/802.1X related parameters for the selected WLAN. • accounting [mode|server|timeout] – Configures RADIUS accounting parameters. • mode [start-interim-stop|start-stop|stop-only] – Sets the WLAN's accounting mode. The options are: • start-interim-stop [interval <60-3600>] – Sets the interval between successive accounting updates between 60 - 3600 seconds. • start-stop – Sends accounting start and stop. • stop-only – Sends accounting stop only. • server [primary|secondary] – Configures the WLAN's primary/secondary RADIUS server. • primary [<A.B.C.D>|<RADIUS-KEY>] – Configures the primary RADIUS server. The authentication is hardcoded to 1813. • secondary [<A.B.C.D>|<RADIUS-KEY>] – Configures the secondary RADIUS server.The authentication is hardcoded to 1813. •<A.B.C.D> – Specify the RADIUS server's IP address (using default port :1813) •radius-key [0 <WORD>|2 <WORD>|<WORD>] – Specify the RADIUS server's shared secret (should not exceeding 127 characters). • timeout <1-300> [retransmit <1-100>] – Sets the time the wireless controller waits for a response from the RADIUS server before retrying accounting. • <1-300> – Specify a time period between 1 - 300 seconds. (default is 5 seconds) •retransmit <1-100> – Sets the number of retries before the switch gives up accounting. Specify a retry count between 1 - 100. (default is 3) • authentication-protocol [chap|pap] – Sets the authentication protocol for RADIUS requests. The options are: • chap – *Challenge Handshake Authentication Protocol* (CHAP) • pap – *Password Authentication Protocol* (PAP) • dscp <0-63> – Specifies a DSCP value to provide QoS to RADIUS packets. The DSCP value must be between 0 - 63.

	• dynamic-authorization [enable] – Configures support for RADIUS dynamic authorization extensions (such as Disconnect Message) and Change-of-Authorization, as described in RFC 3576.
	  • enable – Enables support for RADIUS dynamic authorization.
	• dynamic-vlan-assignment – Assigns users to RADIUS server specified VLANs, instead of only those VLANs mapped to this WLAN.
	  • enable – Enables dynamic/RADIUS-assigned VLAN assignment.
	• mac-auth-format [middle-dash|no-delim|pair-colon|pair-dash|quad-dot] – Sets the MAC address format to use. The options are:
	  • middle-dash – Dash delimiter in the middle - AABBCC-DDEEFF
	  • no-delim – No delimiter - AABBCCDDEEFF
	  • pair-colon – Colon delimiter per pair - AA:BB:CC:DD:EE:FF
	  • pair-dash – Dash delimiter per pair - AA-BB-CC-DD-EE-FF
	  • quad-dot – Dot delimiter per four hex - AABB.CCDD.EEFF
	• mobile-unit [timeout <1-300>] [retransmit <1-100>] – Modifies RADIUS/802.1X supplicant related parameters.
	  • timeout <1-300> – Sets the time, in seconds, the wireless controller waits for a response from the mobile unit before retrying. Specify a value between 1 - 300 seconds.
	  • retransmit <1-100> – Sets the number of retries before the switch gives up and disassociates the mobile unit. Specify a value between 1 -100.
	• reauth <30-65535> – Enables periodic reauthentication of all associated mobile units.
	  • <30-65535> – Specify a reauthentication period between 30 -65536 seconds.
	• server [primary|secondary|timeout] – Modifies RADIUS/802.1X server parameters.
	  • primary [<A.B.C.D>|<RADIUS-KEY>] – Configures the primary RADIUS server. The authentication port is hardcoded to 1812.
	  • secondary [<A.B.C.D>|<RADIUS-KEY>] – Configures secondary RADIUS server. The authentication port is hardcoded to 1812.
	  • <A.B.C.D> – The RADIUS server's IP address (using default port:1812).
	  • radius-key [0 <WORD>|2 <WORD>|<WORD>] – The RADIUS server's shared secret (should not exceed 127 characters).

	• timeout <1-300> – Configures the time, in seconds, the wireless controller waits for a response from the RADIUS server before retrying. • retransmit <1-100> – Configures the number of retries before the wireless controller gives up and disassociates the mobile unit. **Note:** The `RFS7000(config-wireless)# radius server timeout<*> retransmit<*>` should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fallback to the secondary server will not work.
secure-beacon	Does not include this WLAN's SSID in beacon frames.
set-vlan-user-limit [<1-4094>|<VLAN-LIST>]	Sets this WLAN's VLAN user limits. • [<1-4094>|<VLAN-LIST>] <0-8192> – Specifies a single VLAN index between 1 - 4094, or a list of VLANs. Multiple VLANs can be specified as a list (for example,1,3,7) or range (for example, 3-7) of indices. • <0-8192> – Specify the user time limit between 0 - 8192 seconds.
smart-scan-channel [<CHANNEL-LIST>| add <CHANNLE-LIST>| remove <CHANNLE-LIST>]	Specifies a list channels to Motorola Solutions clients to do smart scan. • <CHANNLE-LIST> – A comma-separated list of channels. • add <CHANNLE-LIST> – Adds one or more channels to existing channel list. • remove <CHANNLE-LIST> – Removes one or more channels from existing channel list.
ssid <WLAN-SSID>	Configures this WLAN's SSID. • <WLAN-SSID> – Specify the WLAN's SSID (a string not exceeding 32 characters in length)
storm-control [bcast|macast|ucast]	Enables packet dropping in case of a flooding attack. • bcast [rate-limit <1-1000000>] – Drops broadcast packets. • mcast [rate-limit <1-1000000>] – Drops multicast packets. • ucast [rate-limit <1-1000000>] – Drops unicast packets. • rate-limit <1-1000000> – Rate limits packets. • <1-1000000> – Specify a allowed rate between1 -1000000 packets/sec.
syslog [accounting]	Configures syslog accounting. • accounting [server] – Configures syslog accounting parameters. • server <IP-ADDRESS> – Configures syslog accounting server IP address. • <IP-ADDRESS> – Specify the syslog server's IP address in the A.B.C.D format.
url-log [enable]	Enables HTTP-ALG on WLAN(s).

vlan [<1-4094>|<VLAN-LIST>]	Sets the VLAN assignment of this WLAN. This command starts a new VLAN assignment for given WLAN index. All prior VLAN settings will be erased. • [<1-4094>|<VLAN-LIST>] – Configures the VLAN range list. It can be either a single index or a list (for example, 1,3,7) or range (for example, 3-7) of indices • limit <0-8192> – Optional. Sets user limits on VLANs for this WLAN between 0 - 8192.

Example

```
RFS7000(config-wireless)#wlan 1 aap-proxy-radius enable
Note: aap-radius-proxy must only be enabled when external radius server is usedDo not
enable this feature, when the switch onboard radius server is used.
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 accounting syslog
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 answer-bcast-ess
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 description "TestWLAN"
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 dot11i handshake timeout 2500 retransmit 5
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 dot11i key-rotation enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 dot11i key-rotation-interval 2000
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 hotspot webpage external failure "This feature is under
development"
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 25 mobility enable
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 25 radius accounting timeout 30 retransmit 50
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 25 radius mobile-unit timeout 30 retransmit 5
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 25 ssid TestString
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 1 storm-control bcast rate-limit 1
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 25 syslog accounting server 12.13.14.125 port 5005
RFS7000(config-wireless)#
RFS7000(config-wireless)#wlan 1 url-log enable
RFS7000(config-wireless)#
```

20.1.51 wlan-bw-allocation

Wireless Configuration Commands

Use this command to enable WLAN bandwidth allocation on all radios.

Syntax

```
wlan-bw-allocation [enable]
```

Parameters

enable	Enables WLAN bandwidth allocation on all radios.

Example

```
RFS7000(config-wireless)#wlan-bw-allocation enable
RFS7000(config-wireless)#
```

21

RTLS Instance

Use the `(config-rtls)` instance to configure *Real Time Location System* (RTLS) parameters.

To navigate to this instance, use the command

```
RFSwitch(config)#rtls
RFSwitch(config-rtls)#
```

21.1 RTLS Config Commands

Table 21.1 This table summarizes `config-rtls` commands:

Table 21.1 RTLS Configuration Commands summary

Command	Description	Ref.
aeroscout	Configures AeroScout parameters.	*page 21-2*
ap	Configures AP-specific RTLS parameters.	*page 21-3*
clrscr	Clears the display window.	*page 21-4*
end	Ends the current mode and moves to EXEC mode.	*page 21-5*
exit	Ends current mode and moves to the previous mode.	*page 21-6*
help	Description of the interactive help system.	*page 21-7*
ekahau	Configures ekahau parameters.	*page 21-8*
no	Negates a command or sets its defaults.	*page 21-9*
service	Troubleshoots or debugs `(config-rtls)` instance configurations.	*page 21-11*
show	Displays the running system information.	*page 21-13*
site	Configures site parameters.	*page 21-15*
sole	Configures *Smart Opportunistic Location Engine* (SOLE) parameters.	*page 21-17*
switch	Configures switch parameters.	*page 21-18*

21.1.1 aeroscout

RTLS Config Commands

Use this command to configure support for AeroScout RTLS engine.

Syntax

```
aeroscout [enable|multicast-listen-addr <MAC-ADDRESS>]
```

Parameters

enable	Enables and configures external AeroScout RTLS engine.
multicast-listen-addr <MAC-ADDRESS>	Configures multicast MAC address to which AeroScout tags packets are destined. • <MAC-ADDRESS> – Specify the multicast MAC address in the AA-BB-CC-DD-EE-FF format. The AeroScout's default multicast MAC address is '01:0C:CC:00:00:00'.

Usage Guidelines

Use `[no] aeroscout (enable)` to disable support for Aeroscout RTLS engine. This does not affect on-board locationing.

Example

```
RFSwitch(config-rtls)#aeroscout enable
RFSwitch(config-rtls)#
```

21.1.2 ap

RTLS Config Commands

Use this command to configures AP coordinates.

Syntax

```
ap <MAC> coordinates [x <0-9000>] [y <0-9000>] [z <0-180>]
```

Parameters

<MAC> coordinates
x <0-9000>
y <0-9000>
z <0-180>
	Select a single zone index for configuration
	• <MAC> – Configures access port MAC address.
	  • x <0-9000> – Defines X coordinate
	  • y <0-9000> – Defines Y coordinate
	  • z <0-180> – Defines Z coordinate

Example

```
RFSwitch(config-rtls)#ap AA-BB-CC-DD-EE-FF x 10 y 10 z 0
RFSwitch(config-rtls)#
```

21.1.3 clrscr

RTLS Config Commands

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-rtls)#clrscr
RFSwitch(config-rtls)#
```

21.1.4 end

RTLS Config Commands

Use this command to exit the `(config-rtls)` mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-rtls)#end
RFS7000#
```

21.1.5 exit

RTLS Config Commands

Use this command to end the (`config-rtls)` mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
RFSwitch(config-rtls)#exit
RFSwitch(config)#
```

21.1.6 help

RTLS Config Commands

Use this command to display the interactive help system for the RTLS instance.

Syntax

```
help
```

Parameters

None

Example

```
RFSwitch(config-rtls)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input
(e.g. 'show ve?'.)

RFSwitch(config-rtls)#
```

21.1.7 ekahau

RTLS Config Commands

Use this command to enable and configure the external ekahau location engine.

Syntax

```
ekahau [enable|engine|multicast-listen-addr]

ekahau engine [ip <A.B.C.D>] [port <1000-9000>]

ekahau multicast-listen-addr <MAC-ADDRESS>
```

Parameters

enable	Enables and configures external ekahau RTLS engine.
engine ip <A.B.C.D> [port <1000-9000>]	Configures the external ekahau RTLS engine's IP address and port number. • ip <A.B.C.D> – Configures external location engine's IP address in the A.B.C.D format. • port <1000-9000> – Configures external location engine port between 1000 - 9000.
multicast-listen-addr <MAC-ADDRESS>	Configures multicast MAC address to which ekahau tags packets are destined. • <MAC-ADDRESS> – Specify the multicast MAC address.

Usage Guidelines

Use `[no] enable` and `[no] engine <ip> <port>` commands to undo the ekahau RTLS engine configuration and disable it.

Example

```
RFS7000(config-rtls)#ekahau enable
RFS7000(config-rtls)#

RFS7000(config-rtls)#ekahau engine ip 10.1.1.1 port 1001
RFS7000(config-rtls)#

RFS7000(config-rtls)#ekahau multicast-listen-addr 01-18-8E-00-00-00
RFS7000(config-rtls)#
```

21.1.8 no

RTLS Config Commands

Use this command to negate an RTLS command or set its defaults.

Syntax

```
no [aeroscout|ekahau|service|site|switch|ap]
```

Parameters

no aeroscout [enable| multicast-listen-addr]	Negates AeroScout configuration. • enable – Disables the SOLE adapter. • multicast-listen-addr– Removes configured multicast listening address.
no ekahau [enable|engine| multicast-listen-addr]	Negates ekahau configuration. • enable – Disables aeroscout external engine. • engine – Resets external location engine parameters. • multicast-listen-addr – Removes configured multicast listening address.

no service [filter <1-100>| rtls [mode]]	Negates RFID tag filter configuration.
	• filter <1-100> – Negates RFID tag filter configuration.<1-100> {length|memory-bank|offset} – Negates RFID tag filter configuration for the tag specified by <1-100>. This command negates following tag filter settings:
	  • length – Optional. Length of tag filter
	  • memory-bank – Optional. Tag memory bank
	  • offset – Optional. Offset into the tag memory bank
	• rtls [mode] – Negates the RTLS mode setting.

site [description| dimension| name|scale]	Negates following site configurations: • description – Removes the site description. • dimension – Removes the site dimensions. • name – Removes the site name. • scale – Resets the site scale to default.
ap [<MAC-ADDRESS> <COORDINATES>]	Negates access port location coordinates configuration. • <MAC-ADDRESS> – Specify the access port MAC address in the AA-BB-CC-DD-EE-FF format. • <COORDINATES> – Negates AP location configuration.
switch [coordinates |geo-coordinates]	Negates following switch configuration parameters: • coordinates – Negates switch coordinates configuration within the site. • geo-coordinates – Negates switch geo coordinates configuration.

Usage Guidelines

Use the `no` command to undo the configurations on the parameters mentioned in the table. Refer to the parameters, within this chapter, for complete syntax.

Example

```
RFSwitch(config-rtls)#no aeroscout enable
RFSwitch

RFSwitch(config-rtls)#no ekahau enable
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#no ekahau engine
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#no service inventory 1 zone 1
RFSwitch(config-rtls)#
```

21.1.9 service

RTLS Config Commands

Use this command to troubleshoot or debug the `(config-rtls)` instance configurations.

Syntax

```
service [ap|filter|rtls|show]

service ap <MAC-ADDRESS> [11a-antenna-gain|11bg-antenna-gain] <-20-20>

service filter <1-100> [action|length|mask|memory-bank|name|offset]
service filter <1-100> action [allow|deny]
service filter <1-100> length <1-128>
service filter <1-100> mask <WORD>
service filter <1-100> memory-bank [epc|tid|uid]
service filter <1-100> name <WORD>
service filter <1-100> offset <0-32>

service rtls mode [auto|presence|trilateration]

service show [cli|rtls]
service show rtls [grid|location-history|stats]
service show rtls grid [all|x <0-9000> y <0-9000>]
```

Parameters

ap <MAC-ADDRESS> [11a-antenna-gain| 11bg-antenna-gain]	Configures access port's coordinates.
	• <MAC-ADDRESS> [11a-antenna-gain|11bg-antenna-gain] – Specify the acces port's MAC address in the AA-BB-CC-DD-EE-FF format.
	  • 11a-antenna-gain <-20-20> – Configures 802.11a radio antenna gain.
	  • 11bg-antenna-gain <-20-20> – Configures 802.11bg radio antenna gain.
	  • <-20-20> – Specify the antenna gain between -20 - 20 dBi.

service filter <1-100> [action| length <1-128>| mask|memory-bank| name|offset <0-32>]	Configures following *Radio Frequency Identification* (RFID) tag filter parameters: • <1-100> [action|length|mask|memory-bank|name|offset] – Specify the RFID tag filter's index between 1 - 100. • action [allow|deny] – Configures the action for this tag filter. • allow – Allows RFID tags matching the filter (default). • deny – Denies RFID tags matching the filter. • length <1-128> – Configures the number of bits to compare against the tag mask. • <1-128> – Specify a value between 1 -128. • mask <WORD> – Configures this tag filter's mask. • <WORD> – Specify the tag filter's mask. • memory-bank [epc|tid|uid] – Configures this tag filter's memory bank. The option are: • epc – EPC memory bank • tid – TID memory bank • uid – UID memory bank • name <WORD> – Configures this tag filter's name. • <WORD> – Specify the tag filter's name (should not exceed 32 characters) • offset <0-32> – Configures first (MSB) location of memory bank against which the tag mask is compared. • <0-32> – Specify the first location between 0 -32.
rtls [mode] [auto|presence| trilaterartion]	Configures RTLS mode. • mode [auto|presence|trilateration] – Sets one of the following RLTS modes: • auto – Sets auto mode • presence – Sets presence-only mode • trilateration – Sets trilateration-only mode
show cli	Shows running system information. • cli – Shows CLI tree of current mode.

Usage Guidelines

Use `[no] service [options]` to rollback any service related configurations.

Example

```
RFSwitch(config-rtls)#service filter 1 length 1
RFSwitch(config-rtls)#
```

21.1.10 show

RTLS Config Commands

Use this command to display current system information.

Syntax

```
show <parameters>
```

Parameters

?	Suffix ? to the parameter to view its options and their related configuration details.

Usage Guidelines

Use ? at the end of each option until the final configuration is displayed.

Example

```
RFSwitch(config-rtls)#show ?
  aap-wlan-acl           wlan based acl
  aap-wlan-acl-stats     IP filtering wlan based statistics
  access-banner          Display Access Banner
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  audit-log-filters      Display audit log filter rules
  autoinstall            autoinstall configuration
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  crypto-error-log       Display Crypto Error Log
  crypto-log             Display Crypto Log
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  history                Display the session command history
  interfaces             Interface status
  ip                    Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  redundancy             Configure redundancy group parameters
  role                   Configure role parameters
  rtls                  Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
```

```
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP Redundancy Feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-rtls)#show

RFSwitch(config-rtls)#show rtls ?
  aeroscout       Aeroscout configurations
  espi            ESPI Configuration
  filter          RFID Tag Filters
  ekahau Ekahau configurations
  reference-tags  Reference tag Configurations
  rfid            RFID Configuration
  site            Site configurations
  sole            SOLE configurations
  tags            Tags/Assets (passive, active, wi-fi) Information
  zone            Show zone statistics

RFSwitch(config-rtls)#show rtls

RFSwitch(config-rtls)#show rtls site
Site Name              : Not configured
Site Description       : Not configured
Site Unit              : feet
Site Dimension         : 0L X 0W X 0H
Site Scale Factor      : 1.000000
Switch Coordinates     : 0:0:0
Swith Geo Coordinates  : Not configured
Number of APs          : 0
RFSwitch(config-rtls)#
```

21.1.11 site

RTLS Config Commands

Use this command to configure RTLS site dimensions.

Syntax

```
site [description|dimension|name|scale]

site description <LINE>

site dimension [unit [feet|meters]|x <1-9000> y <1-9000>] {z <0-180>}
site name <WORD>

site scale [<1-90>|auto]
```

Parameters

description <LINE>	Configures the site description. • <LINE> – Enter the site's description.

dimension
[unit [feet|meters]|
x <VALUE>
y <VALUE> [
{z <VALUE>}
	Configures the site dimensions.
	• unit [feet|meters] – Configures the unit for the site dimensions. The options are:
	  • feet – Sets the site dimensions in feet (default).
	  • meters – Sets the site dimensions in meters.
	• x <VALUE> – Configures the site's size on the x-axis (site length).
	  • <VALUE> – The range is <1 -9000> in feet and <1-3000> in meters. Specify the site length between 1 - 9000 feet/1-3000 mtrs.
	• y <VALUE> – Configures the site's size on the y-axis (site width).
	  • <VALUE> – The range is <1 -9000> in feet and <1-3000> in meters. Specify the site width between 1 - 9000 feet/1-3000 mtrs.
	• z <VALUE> – Optional. Configures the site's size on the z-axis (site height).
	  • <VALUE> – The range is <0-180> in feet and <0-60> in meters. Specify the site height between 0 - 180 feet/0 - 60 mtrs.

name <WORD>	Configures the site name. • <WORD> – Specify a name for this site.
scale [<1-90>|auto]	Configures the site scale. The options are: • <1-90> – Configures scale value ranging between1 - 90. • auto – Configures auto scale.

Usage Guidelines

Use `[no] site [description |dimension|name]` to rollback the configurations made using the `site` command

Example

```
RFSwitch(config-rtls)#site description "Motorola RMZ Ecospace,
India, 5th Floor"
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#site name "BLR-RMZ Ecospace"
RFSwitch(config-rtls)#
```

21.1.12 sole

RTLS Config Commands

Use this command to configure *Smart Opportunistic Location Engine* (SOLE) parameters.

This command leads you to the `(config-rtls-sole)#` sub-instance.

Note `sole` command instantiates `(config-rtls-sole)` sub-instance.
For more information, see *Sole Instance on page 23-1*.The prompt changes from `RFSwitch(config-rtls)#` to `RFSwitch(config-rtls-sole)`

Syntax

```
sole
```

Parameters

None

Example

```
RFSwitch(config-rtls)#sole
RFSwitch(config-rtls-sole)#
```

21.1.13 switch

RTLS Config Commands

Use this command to configure the switch's geographical location.

Syntax

```
switch [coordinates|geo-coordinates]

switch coordinates [x <0-65535>] [y <0-65535>] {z <0-65535>}

switch geo-coordinates [longitude <-180.00-80.00>] [latitude <-90.00-90.00>]
```

Parameters

coordinates [x <0-65535> y <0-65535>] {z <0-65535>}	Configures following switch coordinates within the site: • x <0-65535> – Configures X coordinate • y <0-65535> – Configures Y coordinate • z <0-65535> – Optional. Configures Z coordinate
[longitude <-180.00-80.00>] [latitude <-90.00 - 90.00>]	Configures following switch geographic coordinates: • longitude <-180.00-180.00> – Configures the switch's longitude in degrees. • latitude <-90.00-90.00> – Configures switch's latitude., in degrees.

Example

```
RFSwitch(config-rtls)#switch coordinates x 121 y 121 z 135
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#switch geo-coordinates longitude 120 latitude 70
RFSwitch(config-rtls)#
```

22

Role Instance

Use the `(config-role)` instance to configure Role related configuration commands. To navigate to the `config-role` instance, use the following commands:

```
RFSwitch(config)#role <rolename> <rolepriority>
RFSwitch(config-role)#
```

22.1 Role Config Commands

Table 22.1The following table summarizes **`config-role`** commands:

Table 22.1 Command Role Command Summary

Command	Description	Ref.
ap-location	Sets the AP location configuration	*page 22-2*
authentication-type	Sets the authentication type configuration	*page 22-3*
encryption-type	Sets the encryption type	*page 22-4*
essid	Sets ESSID configuration for role based firewall	*page 22-5*
group	Sets role group properties	*page 22-6*
ip	Sets IP configuration properties	*page 22-7*
mac	Sets MAC configuration properties	*page 22-8*
mu-mac	Sets MU MAC configuration properties	*page 22-9*
no	Negates role commands.	*page 22-11*
service	Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations	*page 22-15*
show	Displays the running system information	*page 22-16*
clrscr	Clears the display screen	*page 22-10*
exit	Ends the current mode and moves to the previous mode	*page 22-13*
end	Ends the current mode and moves to the EXEC mode	*page 22-12*
help	Displays the interactive help system in HTML format	*page 22-14*

22.1.1 ap-location

Role Config Commands

Sets the AP location configuration

- This requires the location engine to be enabled on the RF Switch with a site, appropriate zones defined and AP co-ordinates defined. The role based firewall has to know which zone the MU is located when it associates for the ap-parameter option to work.
- The 'ap-location' parameter defines the zone or zones you wish to match.

Syntax

```
ap-location [any|contains|exact|not-contains]
ap-location any
ap-location contains <WORD>
ap-location exact <WORD>
ap_location not-contains <WORD>
```

Parameters

any	Defines any AP location
contains <WORD>	AP location contains the string <WORD>
exact <WORD>	AP location contains the exact string <WORD>
not-contains <word>	AP location does not contain the string <WORD>

Example

```
RFSwitch(config-role)#ap-location any
RFSwitch(config-role)#

RFSwitch(config-role)#ap-location contains office
RFSwitch(config-role)#


RFSwitch(config-role)#ap-location exact warehouse
RFSwitch(config-role)#

RFSwitch(config-role)#ap-location not-contains office
RFSwitch(config-role)#
```

22.1.2 authentication-type

Role Config Commands

Selects authentication type for the role

Syntax

```
authentication-type [any|eq|neq]

authentication-type any

authentication-type eq [eap|hotspot|mac-auth|none]

authentication-type neq[eap|hotspot|mac-auth|none]
```

Parameters

any	Any type of authentication
eq [eap|hotspot|mac-auth|none]	Authentication type equals one of the following: • eap – Extensible Authentication Protocol • hotspot – Hotspot authentication • mac-auth – MAC authentication protocol • none – no authentication used
neq [eap|hotspot|mac-auth|none]	Authentication protocol does not contain one of the listed options

Example

```
RFSwitch(config-role)#authentication-type any
RFSwitch(config-role)#
```

22.1.3 encryption-type

Role Config Commands

Selects encryption for the role

Syntax

```
encryption-type [any|eq|neq]

encryption-type any

encryption-type eq [keyguard|none|wep128|wep128-keyguard|wep64]

encryption-type neq [keyguard|none|wep128|wep128-keyguard|wep64]
```

Parameters

any	Encryption type can be any
eq [keyguard|none|wep128|wep128-keyguard|wep64]	Encryption type equals one of the following: • keyguard • none • wep128 • wep128-keyguard • wep64
neq [keyguard|none|wep128|wep128-keyguard|wep64]	Encryption type must not be one of the listed options

Example

```
RFSwitch(config-role)#encryption-type wep128
RFSwitch(config-role)#
```

22.1.4 essid

Role Config Commands

Sets ESSID configuration for the role

Syntax

```
essid [any|contains|exact|not-contains]
essid any
essid contains <WORD>
essid exact <WORD>
essid not-contains <WORD>
```

Parameters

any	Any ESSID
contains <WORD>	ESSID contains the string <WORD>
exact <WORD>	ESSID contains the exact string <WORD>
not-contains <word>	ESSID does not contain the string <WORD>

Example

```
RFSwitch(config-role)#essid any
RFSwitch(config-role)#
```

22.1.5 group

Role Config Commands

Sets group configuration for the role

Syntax

```
group [any|contains|exact|not-contains]

group any

group contains <WORD>

group exact <WORD>

group not-contains <WORD>
```

Parameters

any	Any group
contains <WORD>	Group contains the string <WORD>
exact <WORD>	Group contains the exact string <WORD>
not-contains <word>	Group does not contain the string <WORD>

Example

```
RFSwitch(config-role)#group any
RFSwitch(config-role)#
```

22.1.6 ip

Role Config Commands

Sets IP parameters for the role

Syntax

```
ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<WORD>] [in|out] acl-precedence <1-100>
```

Parameters

access-group [<1-99>| <100-199>|<1300-1999>| <2000-2699>|<WORD>] [in|out] acl-precedence <1-100>	Sets the ACL precedence for the following ACL List entries • <1-99> – IP standard access list • <100-199> – IP extended access list • <1300-1999> – IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <word> – IP access list name • in – Apply grouping to incoming packets • out – Apply grouping to outgoing packets • acl-precedence <1-100> – Sets ACL precedence to a value between 1 and 100

Example

```
RFSwitch(config-role)#ip access-group 8 in acl-precedence
RFSwitch(config-role)#
```

22.1.7 mac

Role Config Commands

Sets MAC access group configuration commands

Syntax

```
mac access-group <WORD> [in|out] acl-precedence <1-100>
```

Parameters

access-group <word> [in|out] acl-precedence <1-100>	Sets MAC access group configuration parameters • <WORD> – The ACL name • in – Apply grouping to incoming packets • out – Apply grouping to outgoing packets • acl-precedence <1-100> – sets ACL precedence to a value between 1 and 100

Example

```
RFSwitch(config-role)#mac access-group 8 in acl-precedence
RFSwitch(config-role)#
```

22.1.8 mu-mac

Role Config Commands

Configures the MU MAC addresses for role based firewall

Syntax

```
mu-mac [<MAC Address>|<MAC Address>/<Mask>|any]
```

Parameters

<MAC Address>	The address of the MU that is allowed. MAC address can be in the format AA:BB:CC:DD:EE:FF or AA-BB-CC-DD-EE-FF or AABB.CCDD.EEFF.
<MAC Address>/<Mask>	The address and mask combination for the mu to be allowed. <MAC Address> and <Mask> should be in the format AA:BB:CC:DD:EE:FF or AA-BB-CC-DD-EE-FF or AABB.CCDD.EEFF.
any	Match with any MAC address

Example

```
RFSwitch(config-role)#mu-mac aa:bb:cc:dd:ee:ff
RFSwitch(config-role)#
```

22.1.9 clrscr

Role Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-role)#clrscr
RFSwitch(config-role)#
```

22.1.10 no

Role Config Commands

Negates role commands

Syntax

```
no [ap-location|authentication-type|encryption-type|essid|
group|ip|mac|mu-mac]

no ap-location
no authentication-type
no encryption-type
no essid
no group
no ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<WORD>] [in|out] acl-precedence <1-100>
no mac <WORD> [in|out] acl-precedence <1-100>
no mu-mac
```

Parameters

None

Example

```
RFSwitch(config-role)#no ap-location
RFSwitch#
```

22.1.11 end

Role Config Commands

Exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Syntax

```
end
```

Parameters

None

Example

```
RFSwitch(config-role)#end
RFSwitch#
```

22.1.12 exit

Role Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch#(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
RFSwitch(config-role)#exit
RFSwitch(config)#
```

22.1.13 help

Role Config Commands

Displays the system's interactive help in HTML format

Syntax

```
help
```

Parameters

None

Example

```
RFSwitch(config-role)#help
  CLI provides advanced help feature.  When you need help,
  anytime at the command line please press '?'.

  If nothing matches, the help list will be empty and you must backup
  until entering a '?' shows the available options.
  Two styles of help are provided:
  1. Full help is available when you are ready to enter a
     command argument (e.g. 'show ?') and describes each possible
     argument.
  2. Partial help is provided when an abbreviated argument is entered
     and you want to know what arguments match the input
     (e.g. 'show ve?'.)

  RFSwitch(config-dhcp)#
```

22.1.14 service

Role Config Commands

Invokes service commands to troubleshoot or debug (config-role) instance configurations

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-role#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-class
  +-WORD [class WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
   +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
.......................
.....................................................
RFSwitch(config-dhcp)#
```

22.1.15 show

Role Config Commands

Displays current system information

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-role)#show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
RFSwitch(config-role)#
```

23

Sole Instance

Use the `(config-sole)` instance to configure SOLE related configuration commands.

To navigate to this instance, ues the following commands:

```
RFS7000(config)#rtls
RFS7000(config-rtls)#sole
RFS7000(config-rtls-sole)#
```

23.1 Sole Config Commands

Table 23.1 summarizes `config-sole` commands:

Table 23.1 SOLE Config Command Summary

Command	Description	Ref.
aap-rssi-update-interval	Configures AAP probe packet interval.	*page 23-2*
clrscr	Clears the display screen.	*page 23-3*
end	Ends the current mode and moves to the EXEC mode.	*page 23-4*
exit	Ends the current mode and moves to the previous mode.	*page 23-5*
help	Describes the interactive help system.	*page 23-6*
locate	Invokes location commands.	*page 23-7*
mobile-unit	Sets the mobile-unit configurations	*page 23-8*
no	Negates a command or sets defaults values	*page 23-8*
service	Troubleshoots or debugs `the (config-sole)` instance configuration.	*page 23-12*
show	Displays running system information.	*page 23-13*

23.1.1 aap-rssi-update-interval

Sole Config Commands

Use this command to configure AAP probe packet interval.

Syntax

```
aap-rssi-update-interval <5-3600>
```

Parameters

<5-3600>	Specify the interval between 5 - 3600 seconds.

Example

```
RFS7000(config-rtls-sole)#aap-rssi-update-interval 5
RFS7000(config-rtls-sole)#
```

23.1.2 clrscr

Sole Config Commands

Use this command to clear the Display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
RFS7000(config-rtls-sole)#clrscr
RFS7000(config-rtls-sole)#
```

23.1.3 end

Sole Config Commands

Use this command to end the (`config-rtls-sole`) mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`

Syntax

```
end
```

Parameters

None

Example

```
RFS7000(config-rtls-sole)#end
RFS7000#
```

23.1.4 exit

Sole Config Commands

Use this command to end (`config-rtls-sole`) mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
RFS7000(config-rtls-sole)#exit
RFS7000(config-rtls)#
```

23.1.5 help

Sole Config Commands

Use this command to display the interactive help system for SOLE instance.

Syntax

```
help
```

Parameters

None

Example

```
RFS7000(config-rtls-sole)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-rtls-sole)#
```

23.1.6 locate

Sole Config Commands

Use this command to invoke location commands.

Syntax

```
locate [aeroscout|ekahau|mobile-unit]

locate aeroscout [enable|interval <5-3600>]
locate ekahau [enable|interval <5-3600>]
locate mobile-unit [<MAC-ADDRESS> [enable]|enable|interval <5-3600>]
```

Parameters

aeroscout [enable| interval <5-3600>]	Locates AeroScout tags. • enable – Starts locating AeroScout tags. • interval <5-3600> – Configures the interval at which tag locating is performed. • <5-3600> – Specify a value between 5 - 3600 seconds.
ekahau [enable| interval <5-3600>]	Locates ekahau tags. • enable – Starts locating ekahau tags. • interval <5-3600> – Configures the interval at which tag locating is performed. • <5-3600> – Specify a value between 5 - 3600 seconds.
mobile-unit [<MAC-ADDRESS>| enable| interval <5-3600>]	Locates specified mobile units • <MAC-ADDRESS> [enable] – Specify the MAC address of the mobile unit in the AA-BB-CC-DD-EE-FF format. • enable – Starts locating the spcified mobile unit. • enable – Starts locating mobile units. • interval <5-3600> – Configures the interval at which tag locating is performed. • <5-3600> – Specify a value between 5 - 3600 seconds.

Example

```
RFS7000(config-rtls-sole)#locate aeroscout enable
RFS7000(config-rtls-sole)#

RFS7000(config-rtls-sole)#locate ekahau interval 5
RFS7000(config-rtls-sole)#
```

23.1.7 mobile-unit

Sole Config Commands

Use this command to configure amobile unit's power level.

Syntax

```
mobile-unit [power-level <1-100>]
```

Example

power-level <1-100>	Specifies the mobile unit's power level between 1 - 100 dBm.

```
RFS7000(config-rtls-sole)#mobile-unit power-level 2
RFS7000(config-rtls-sole)#
```

23.1.8 no

Sole Config Commands

Use this commnad to negate a SOLE command or set its defaults.

Syntax

```
no [aap-rssi-update-interval|locate|mobile-unit|redundancy|rssi-filter]
```

Parameters

no aap-rssi-update-interval	Negates AAP probe packet interval configurations.
no locate [aeroscout| ekahau| mobile-units]	Negates locationing • aeroscout – Negates locating AeroScout tags • ekahau – Negates locating ekahau tags • mobile-units – Negates locating specified mobile units
no mobile-units [power-level]	Negates mobile unit power level configuration.
no redundancy [enable]	Negates SOLE redundancy configuration.
no rssi-filter	Sets *Received Signal Strength Indicator* (RSSI) filter to default.

Example

```
RFS7000(config-rtls-sole)#no aap-rssi-update-interval
RFS7000(config-rtls-sole)#

RFS7000(config-rtls-sole)#mobile-unit power-level 2
RFS7000(config-rtls-sole)#
```

23.1.9 redundancy

Sole Config Commands

Use this command to enable SOLE redundancy.

Syntax

```
redundancy (enable)
```

Parameters

enable	Enables SOLE redundancy

Example

```
RFS7000(config-rtls-sole)#redundancy enable
RFS7000(config-rtls-sole)#
```

23.1.10 rssi-filter

Sole Config Commands

Use this command to filter rssi values below this threshold.

Syntax

```
rssi-filter <-100-0>
```

Parameters

<-100-0>	Specify the RSSI filter value between -100 - 0 dbm.

Example

```
RFS7000(config-rtls-sole)#rssi-filter -100
RFS7000(config-rtls-sole)#
```

23.1.11 service

Sole Config Commands

Use this commnad to invoke service commands to troubleshoot or debug `(config-sole)` instance configurations.

Syntax

```
service [show] [cli]
```

Parameters

show cli	Show running system information • cli – Show CLI tree of current mode

Example

```
RFS7000(config-rtls-sole)#service show cli
Location Engine Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>'
]
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-sa
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>'
]
      +-vlan
        +-<1-4094> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-409
4>']
      +-all [show ip access-group all]
      +-role [show ip access-group role ( WORD | )]
RFS7000(config-rtls-sole)#
```

23.1.12 show

Sole Config Commands

Use this command to display current system information.

Syntax

```
show <parameter>
```

Parameters

?	Suffix ? to the parameter to view its options and their related configuration details

Example

```
RFS7000(config-rtls-sole)#show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-banner         Display Access Banner
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  audit-log-filters     Display audit log filter rules
  autoinstall           autoinstall configuration
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  crypto-error-log      Display Crypto Error Log
  crypto-log            Display Crypto Log
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Configure redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
```

```
    timezone              Display timezone
    traffic-shape         Display traffic shaping
    upgrade-status        Display last image upgrade status
    users                 Display information about currently logged in users
    version               Display software & hardware version
    virtual-ip            IP Redundancy Feature
    wireless              Wireless configuration commands
    wlan-acl              wlan based acl

RFS7000(config-rtls-sole)#
```

Appendix A - Customer Support

Motorola Solutions Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support at *https://portal.motorolasolutions.com/Support/US-EN*

When contacting Enterprise Mobility support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Motorola Solutions responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola Solutions business partner, contact that business partner for support.

Customer Support Web Site

MotorolaSolutions' Support Central Web site, located at *https://portal.motorolasolutions.com/Support/US-EN* provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Manuals

https://portal.motorolasolutions.com/Support/US-EN

General Information

Obtain additional information by contacting Motorola Solutions at:

1-800-722-6234, inside North America

+1-516-738-5200, in/outside North America

http://www.motorolasolutions.com/

MOTOROLA Solutions INC.
1301 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196-1078, U.S.A.
http://www.motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA Solutions and the Stylized M logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are a properties of their owners.
©2014 Motorola Solutions, Inc. All rights reserved.

72E-161313-01 Revision B
March 2014